SIEMENS

SIMATIC NET

Network management SINEMA Server

Operating Instructions

04/2019

C79000-G8976-C241-10

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C241-10
℗ 04/2019 Subject to change

Preface

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SINEMA, SCALANCE, SIMATIC

Purpose of this documentation

This manual will help you install, configure and operate the application, SINEMA Server. It contains basic information about devices, protocols, security mechanisms and other properties of industrial networks and provides guidance and advice on monitoring and evaluating them.

Validity of the manual

The information in this document applies to the SINEMA Server V14 SP2 software.

New in this product version

Revision of the content and editorial revision.

New functions, including:

- Syslog client functionality

Expansion of existing functions, including:

- View-specific validation reports
- Analysis of password strength when creating new passwords
- Revised behavior when exchanging device profiles between SINEMA Server instances
- Improved usability when working with topology representations
- Enhanced filter options for event lists
- Optional exclusion of devices from PROFINET discovery
- Improved behavior for SNMP authentication on devices
- Advanced configuration of user permissions
- Revised behavior for determining the connection type of devices

Further information

You will find additional and updated information about SINEMA Server on the Internet. The Siemens Automation Customer Support Web site contains manuals, FAQs and software updates among other content. You can access this information via the following link:

SINEMA server (https://support.industry.siemens.com/cs/ww/en/ps/15393)

The figures in this manual may differ in color from the design of the web interface.

Allowance for network utilization by SINEMA Server

To monitor devices, SINEMA Server uses part of the data transfer rate available in the network. This must be taken into account when planning networks in which SINEMA Server will be used.

License conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product. The acceptance of the disclaimers of liability and warranty it contains is a clear precondition of the use of open source software.

You will find license conditions in the following document on the supplied data medium:

- OSS_SINEMAServer_99.pdf

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary on the Internet at the following address:

50305045 (https://support.industry.siemens.com/cs/ww/en/view/50305045)

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
Link: (https://www.siemens.com/industrialsecurity)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are

available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
Link: (https://www.siemens.com/industrialsecurity)

Security recommendations

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to make sure that this product meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Keep the software you are using up to date. Check regularly for security updates for the product.

  You will find information on this at http://www.siemens.com/industrialsecurity.
- Only activate protocols you require to monitor the devices.
- Whenever possible, always use the variants of protocols that provide greater security (e.g. SNMPv3, HTTPS etc.).
- Restrict access to the SINEMA Server to qualified personnel.

SINEMA Server clients

- It is strongly recommended that you use the HTTPS protocol for access to the Web user interface of SINEMA Server. The data is transferred encrypted and cannot be read by unauthorized third persons.
- It is strongly recommended that you use the OPC UA protocol for access via OPC. The OPC UA protocol is more secure than the OPC DA protocol.
- Users who access functions of SINEMA Server by calling URLs, should only be assigned the absolutely necessary rights.
- Keep the Web browser you are using up to date on the clients.

Passwords

- Define rules for the use of the software and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Change all default passwords for users before you use the software.
- Only use passwords with a high password strength. Avoid weak passwords for example password1, 123456789, abcdefgh.

- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems or after it has expired.

Keys and passwords

This section deals with the security keys and certificates you require to set up SSL.

- We strongly recommend that you create your own SSL certificates and make them available.

  How you generate HTTPS certificates is described in the following section of this manual: Port settings (Page 32)
- We recommend that you use certificates with a key length of 2048 bits.

Automation License Manager

If you do not require the network functions of the Automation License Manager, deny access to these functions in your firewall.

Assumptions

We assume the following situation:

- SINEMA Server, monitored devices and OPC clients are protected by a firewall.
- It is certain that access to the SINEMA Server via the Internet is only possible using security mechanisms such as SSL-VPN.

Table of contents

Network management with SINEMA Server - introduction

1

1.1 Area of application and functions

The complexity and the number of nodes in Ethernet-based production networks are growing constantly due to increasing requirements. The failure of individual devices in such networks can mean loss of production and, in the worst case, bring the production chain to a standstill. To minimize unproductive times and the resulting costs, transparency of networks with continuous network monitoring is indispensable.

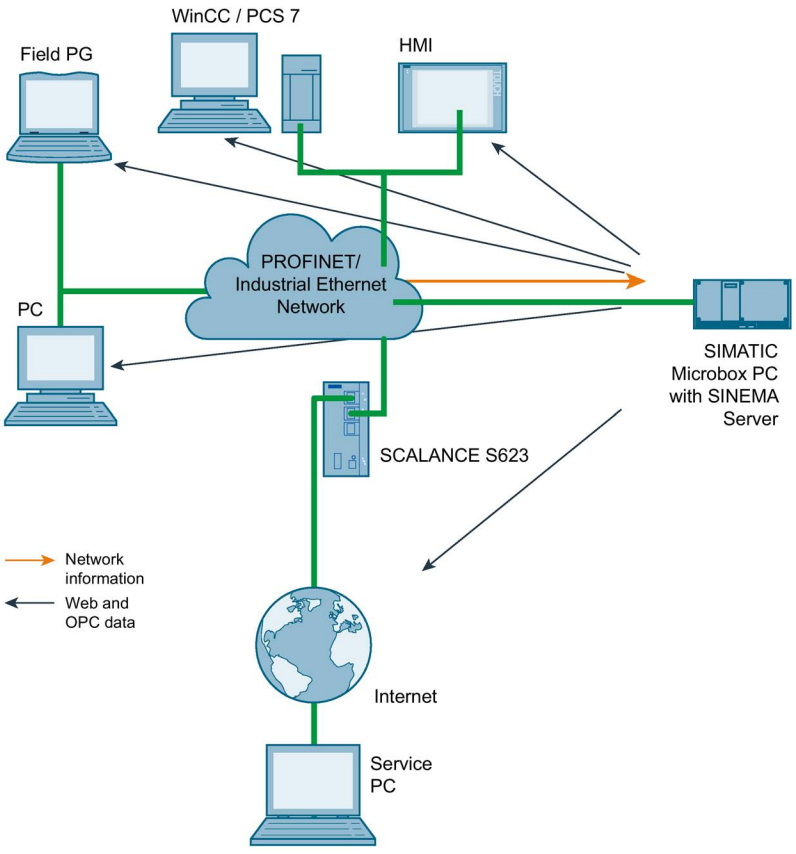
The network management software SINEMA Server is designed specifically for the requirements of industrial communication and monitors devices in the network such as:

- the programmable controllers and wireless devices connected to LANs or WLANs
- the infrastructure components such as Industrial Ethernet switches or access points of industrial WLANs.

With the help of extensive diagnostics and reporting functions, SINEMA Server ensures that network problems are recognized early and can be dealt with.

Integration of SINEMA Server

The following graphic is a schematic representation of the integration of SINEMA Server in a network to be monitored.



- Management station with SINEMA Server

  The SINEMA Server application runs on a SIMATIC Microbox or on a PC. The device on which the SINEMA Server runs is known as the management station. The management station is a node in the network to be monitored.

- Web client for accessing SINEMA Server

  Access to the Web server of SINEMA Server is via Web browser on the clients. A Web client can also be operated on the management station itself.

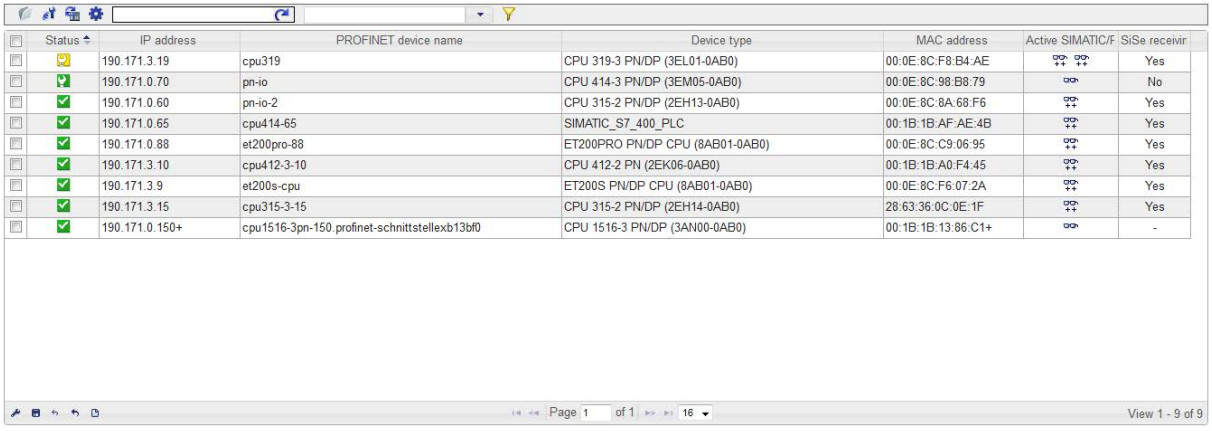
- OPC server

  For OPC applications, you have an additional interface available to the SINEMA Server network data. HMI systems such as SIMATIC WinCC also use this option for access to network data.

1.2 Overview of the program functions

Automatic device detection

SINEMA Server discovers devices in the network automatically and obtains their device information. Cyclically, SINEMA Server polls the overall status of every discovered device and highlights this in color.



Status	IP address	PROFINET device name	Device type	MAC address	Active SIMATIC/F	SiSe receivir
	190.171.3.19	cpu319	CPU 319-3 PN/DP (3EL01-0AB0)	00:0E:8C:F8:B4:AE		Yes
	190.171.0.70	pn-io	CPU 414-3 PN/DP (3EM05-0AB0)	00:0E:8C:98:B8:79		No
	190.171.0.60	pn-io-2	CPU 315-2 PN/DP (2EH13-0AB0)	00:0E:8C:8A:68:F6		Yes
	190.171.0.65	cpu414-65	SIMATIC_S7_400_PLC	00:1B:1B:AF:AE:4B		Yes
	190.171.0.88	et200pro-88	ET200PRO PN/DP CPU (8AB01-0AB0)	00:0E:8C:C9:06:95		Yes
	190.171.3.10	cpu412-3-10	CPU 412-2 PN (2EK06-0AB0)	00:1B:1B:A0:F4:45		Yes
	190.171.3.9	et200s-cpu	ET200S PN/DP CPU (8AB01-0AB0)	00:0E:8C:F6:07:2A		Yes
	190.171.3.15	cpu315-3-15	CPU 315-2 PN/DP (2EH14-0AB0)	28:63:36:0C:0E:1F		Yes
	190.171.0.150+	cpu1516-3pn-150.profinet-schnittstellexb13bf0	CPU 1516-3 PN/DP (3AN00-0AB0)	00:1B:1B:13:86:C1+		-

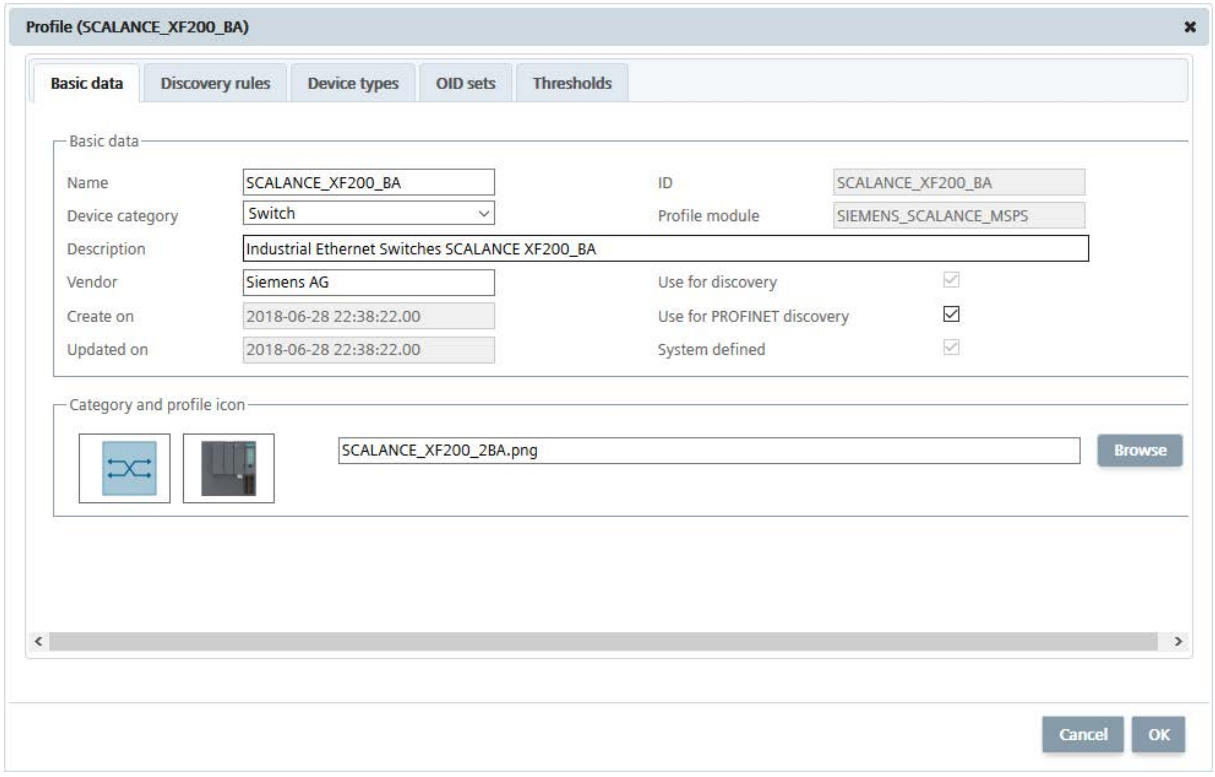
Page 1 of 1 16 View 1 - 9 of 9

For more detailed information, refer to the following sections:

- Device discovery: Detecting devices in the network (Page 49)
- Determining overall device statuses: Administration - Events Overall status groups (Page 200)

Device display with device profiles

The display schemes for devices discovered in SINEMA Server are specified in so-called device profiles that are assigned to the devices automatically when they are discovered by SINEMA Server. If a device has been assigned to a device profile, it is displayed with the device details stored in the relevant device profile.



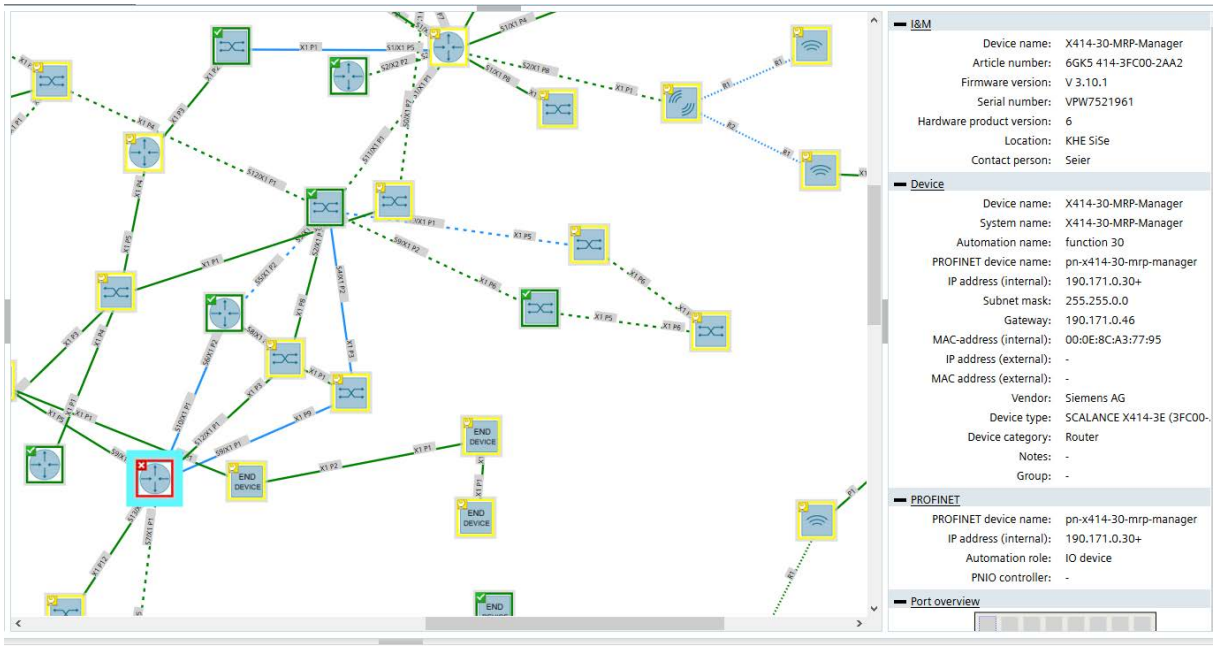
Device profiles access the information of devices via SNMP and SIMATIC / PROFINET. Devices supported by device profiles include SCALANCE W, SCALANCE X and SCALANCE S, SIMATIC CPUs 300/400/1200/1500 and SIMATIC NET CPs 200/300/400. The more than 220 standard device profiles cover more than 2000 Siemens devices. When necessary, the Profile editor can be used to create your own device profiles based on existing device profiles.

For more detailed information on device profiles, refer to the following sections:

- Setting up network devices individually - using the Profile editor (Page 53)
- Administration - Discovery / Profiles (Page 177)

Network monitoring with network topologies

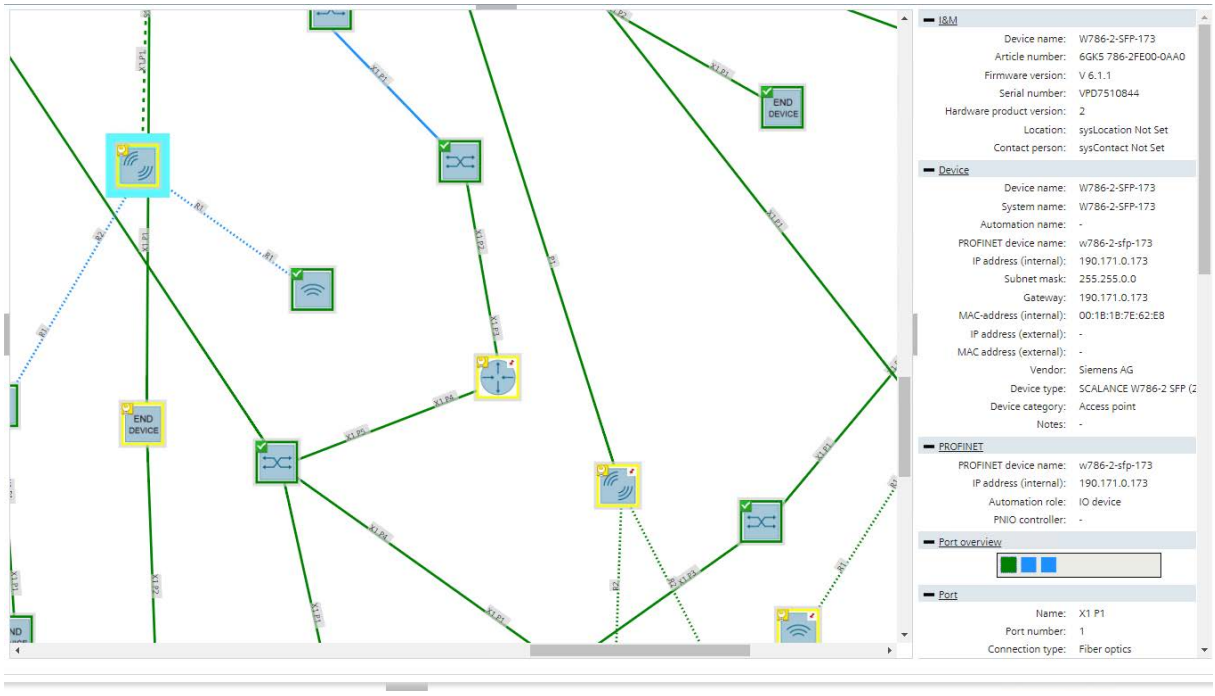
The device information discovered by SINEMA Server also includes the information about the neighboring devices. With the help of the SNMP and/or PROFINET protocols, SINEMA Server reads out the neighborhood information and calculates a topology display using the LLDP protocol in which the detected connections between devices are shown. To monitor the devices, expected statuses for devices involved, connectors, and connections can be defined in the topology display. Deviations between detected statuses and configured setpoint statuses are highlighted by SINEMA Server.



For more information, refer to the section Topology (Page 134).

User-specific network monitoring

The number and appearance of the devices visible in SINEMA Server can be configured for specific users. To achieve this, you can define sections of the network monitoring as views by assigning the devices to be monitored to the views.



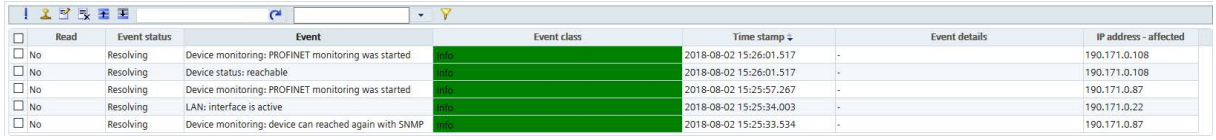
For each view, an additional topology display can be generated in which the assigned devices can be freely arranged and networked. You then assign the created views to the required users.

You will find more detailed information on views and assigning users in the following sections:

- Setting up and using views (Page 61)
- Views (Page 125)
- Administration - User (Page 208)

Events

Events such as changes to the accessibility status of a monitored device are recorded by SINEMA Server and stored in an event database. This enables the evaluation of historical events.



Read	Event status	Event	Event class	Time stamp	Event details	IP address - affected
No	Resolving	Device monitoring: PROFINET monitoring was started	Info	2018-08-02 15:26:01.517	-	190.171.0.108
No	Resolving	Device status: reachable	Info	2018-08-02 15:26:01.517	-	190.171.0.108
No	Resolving	Device monitoring: PROFINET monitoring was started	Info	2018-08-02 15:25:57.267	-	190.171.0.87
No	Resolving	LAN: interface is active	Info	2018-08-02 15:25:34.003	-	190.171.0.22
No	Resolving	Device monitoring: device can reached again with SNMP	Info	2018-08-02 15:25:33.534	-	190.171.0.87

As default, SINEMA Server includes predefined events for important status changes in the network that can, when necessary, be expanded with new events. Apart from the event

texts, the reaction to events, for example calling a program or sending an e-mail can also be configured. The influence of events on the overall statuses of monitored devices can be adapted by including them in overall status groups.

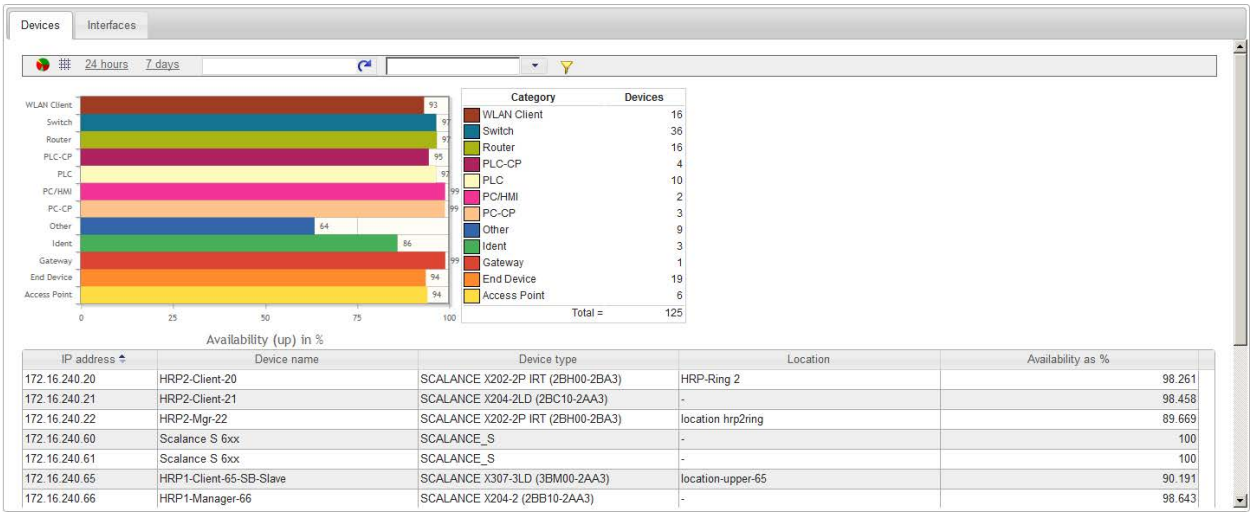
Triggered events can be forwarded from SINEMA Server to up to three Syslog servers.

For more detailed information on event class and overall status groups, refer to the following sections:

- Events: Configuring event reactions - displaying events (Page 58)
- Overall status groups: Administration - Events Overall status groups (Page 200)
- Syslog server configuration: Administration - Events Syslog Server (Page 207)

Creating reports

With the report function, you obtain exportable evaluations of the network monitoring in both textual and graphic form.

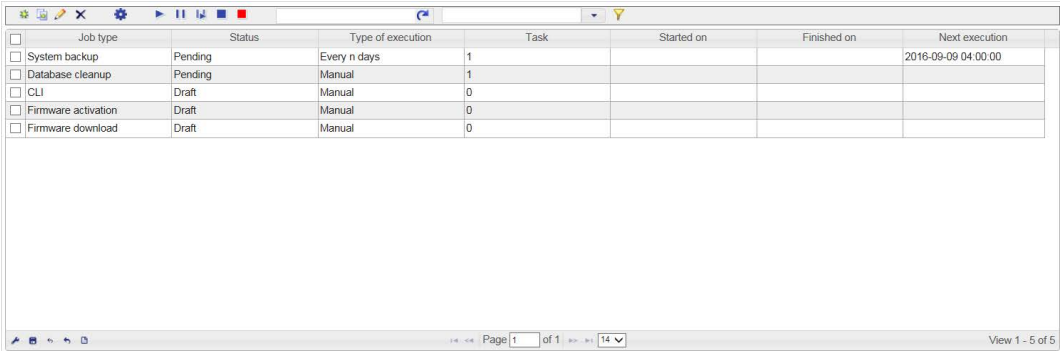


IP address	Device name	Device type	Location	Availability as %
172.16.240.20	HRP2-Client-20	SCALANCE X202-2P IRT (2BH00-2BA3)	HRP-Ring 2	98.261
172.16.240.21	HRP2-Client-21	SCALANCE X204-2LD (2BC10-2AA3)	-	98.458
172.16.240.22	HRP2-Mgr-22	SCALANCE X202-2P IRT (2BH00-2BA3)	location hrp2ring	89.669
172.16.240.60	Scalance S 6xx	SCALANCE_S	-	100
172.16.240.61	Scalance S 6xx	SCALANCE_S	-	100
172.16.240.65	HRP1-Client-65-SB-Slave	SCALANCE X307-3LD (3BM00-2AA3)	location-upper-65	90.191
172.16.240.66	HRP1-Manager-66	SCALANCE X204-2 (2BB10-2AA3)	-	98.643

For more detailed information on reports, refer to the section Reports (Page 149)

Execution of jobs

Jobs allow you to perform management tasks such as firmware downloads to SCALANCE X / SCALANCE W / SCALANCE M800 / SCALANCE S615 devices, system backups and database cleanups. These can be started time-controlled or manually and allow work with other functions of SINEMA Server while they are executing.



For more detailed information on jobs, refer to the section Administration - Jobs (Page 220)

Creating validation reports

Validation reports are available to check whether certain device properties such as firmware versions or PROFINET device names currently deviate from a specification. The validations to be performed in a validation report can be put together freely and prioritized in terms of the validation result.

Validation reports are generated as PDF files and document the validation result as well as the cause of validations that are not passed.

Validation overview..... FAILED

Co-worker: Administrator

Department / company: Siemens AG

-

Device properties:

Validation	Validated	Obligatory	Checked	Affected	Result
White list for firmware versions	Yes	Yes	12 (19)	-	Passed
Different firmware versions	Yes	Yes	12 (19)	-	Passed
IP address parameters	Yes	Yes	12(19)	1	Failed
Device names	No	-	-	-	-
Duplicate MAC addresses	No	-	-	-	-
Duplicate IP addresses	No	-	-	-	-

PROFINET:

Validation	Validated	Obligatory	Checked	Affected	Result
Duplicate PROFINET device names	No	-	-	-	-
PROFINET IO devices without assigned controller	Yes	Yes	12(19)	2	Failed

Performance (devices):

Validation	Validated	Obligatory	Checked	Affected	Result
Device availability	Yes	Yes	12 (19)	-	Passed

Performance (ports):

Validation	Validated	Obligatory	Checked	Affected	Result

For more detailed information on validation reports, refer to the section Reports - validation reports (Page 159)

Installing, setting up and calling SINEMA Server 2

2.1 Performance characteristics of SINEMA Server

Features of the Web interface

The Web interface of SINEMA Server can be used by several clients at the same time to access network information.

Access to the SINEMA Server Web interface is possible using an unencrypted HTTP connection or an encrypted HTTPS connection. User authentication using a user name and password increases the security against unauthorized access.

Regardless of their location in the network, several users can access the same information at the same time.

Configuration limits of SINEMA Server

The number of monitored network devices is limited within the framework of the licensing levels. See section License information (Page 22).

A maximum of 500 network devices can be monitored.

For each management station, SINEMA Server supports remote access by ten users simultaneously. This means that an installation of SINEMA Server can be used by up to ten users at the same time for remote monitoring of network operation.

Further features

In addition to the descriptions in the previous sections, SINEMA Server also provides the following additional functions:

- Forwarding of network data and alarms to other systems using an e-mail client function.
- Users with access to SINEMA Server can also use the OPC server to display device data acquired by SINEMA Server.
- The export function allows the configuration data of SINEMA Server to be archived. Similarly, the configuration data can also be imported into SINEMA Server.
- Capability of integration in HMI systems (HMI - Human Machine Interface) and visualization systems such as SIMATIC WinCC. This makes the monitoring of communication possible in a process visualization system.
- Using a CSV export function (filtered) data of all lists can be downloaded, refer to the section Calling functions with a URL (Page 81)

2.2 Installing and uninstalling software

2.2.1 License information

To use this application, you require a SINEMA Server license.

Trial license

The application ships with a trial license. The SINEMA Server application automatically generates a trial license. The trial license can be extended by upgrading to a new license type.

License types and corresponding configuration limits

The following seven license types are available for SINEMA Server:

- License type 500: This license supports up to 500 monitored devices
- License type 250: This license supports up to 250 monitored devices.
- License type 100: This license supports up to 100 monitored devices.
- License type 50: This license supports up to 50 monitored devices.
- Update license (available as of SINEMA Server V12): Detects the existing license type and upgrades it to the higher SINEMA Server version.
- Emergency: This license supports up to 500 monitored devices.

  If a license type is damaged or corrupted, an emergency license can be used. The emergency license provides validity for a further 14 days.
- Trial 500: This license is a trial license and supports up to 500 monitored devices. The following restrictions apply as compared to the full version:
  - Causes for results of validation reports are not displayed, and it is also not possible to generate pictures of the topology display.
  - Only one device can be processed at a time with jobs for firmware downloads and for executing CLI scripts.

Note

Management station is not included in the configuration limits

The configuration limits specified by a license type do not include the network adapters of the management station.

Note

Trial 500 license

The Trial 500 license is only valid for 21 days. Once the trial version has been activated on the computer it cannot be activated again.

Note

Starting up the first time without a license key

If you launch SINEMA Server the first time without a valid license key, the application setup automatically installs and activates this trial license on your computer.

Note

Passively monitored devices

Devices in the monitoring status "Passively monitored" do not require a device license since these are monitored solely by the assigned controller.

Automation License Manager

To manage your SINEMA Server license, you use the Automation License Manager (ALM) program. This program is used to manage the license keys. Software products that require license keys automatically indicate this requirement to the Automation License Manager. If the ALM finds a valid license key for the software, this can be used according to the end user license agreement.

After installing SINEMA Server, you can call up the documentation for the Automation License Manager. To do this, select **Start > All Programs >Siemens Automation > Documentation** in the Windows menu.

Storage location for license keys

You can store license keys on storage devices such as license key sticks, exchangeable drives (however not on optical memory media such as CD or DVD) or on USB memory sticks. To be able to use SINEMA Server productively, the license keys must, however, be stored locally on your computer.

Defining monitored devices according to license type

All devices detected by SINEMA Server are displayed in the device list. If SINEMA Server detects more devices than the active license type allows, the devices are monitored in the order in which they are detected by SINEMA Server. Devices that are detected after reaching the maximum number of devices with the license type are only displayed in the device list and cannot be monitored. From the toolbar of the device list, you can disable monitoring for devices that are not required and enable it for devices that are required, see section Device window with device list (Page 96). Alternatively, you can perform a license update.

License update

To extend the license or to expand to a higher number of monitored devices, you require an update to a new license. To allow the license update to be made, the Automation License Manager requires access to the license key of the update license. The Automation License Manager or SINEMA Server then detects the update license automatically.

License types 50/100/250 can be combined. The license type is expanded according to the addition. However, only a maximum of 500 devices can be monitored. If more than 500 devices need to be monitored, these additional devices can be monitored by a separate management station. To monitor devices that are monitored by different management stations, the server overview function can be used.

Note

Configuration limits of the current version

The current version of SINEMA Server supports a maximum of 500 devices.

With a license update, you can also update to a higher version of SINEMA Server.

To run such a license update, follow the steps outlined below:

1. In the Automation License Manager, select the **"View > Management"** menu command.
2. In the navigation area, select the storage location of the license key with which you want to perform the update.
3. In the object area, select the license key with which the update will be performed.
4. Select the **"License key > Upgrade..."** menu commands.

License downgrade

A license downgrade is possible if you have at least one license type available. For the downgrade, you do, however, require a license type higher than 50. If, for example, you have license type 50 + license type 50 (two licenses) it is only possible to downgrade to one license.

NOTICE

Checking the number of monitored devices

Before performing the license downgrade, make sure that the number of monitored devices does not exceed the number of monitored devices that will be licensed following the downgrade.

Otherwise, a login will no longer be possible following the license downgrade. In this case, run a license update with a suitable number of devices.

To perform a downgrade with a license type, follow the steps outlined below:

1. Stop SINEMA Server and its services. To do this, you can use the "SINEMA Server Monitor" window.
2. In the Automation License Manager, select the **"View > Management"** menu command.

3. In the navigation area, select the storage location of the license key with which you want to perform the downgrade.
4. Select the **"License key > Transfer..."** menu command to transfer the license key to another user.

NOTICE
Checks on completion of the license downgrade Following the downgrade, there must still be at least one license remaining in the navigation area.

2.2.2 Installing SINEMA Server - requirements and procedure

Overview

Most of the installation is handled automatically. The SETUP routine itself recognizes whether other program components apart from SINEMA Server itself need to be installed. The installation routine takes the required actions as necessary.

Successful installation and problem-free operation of SINEMA Server require the following system properties:

Hardware requirements

Parameter	Minimum requirements	Recommended requirements	Minimum requirements with VMware ESXi V6.7	Recommended requirements with VMware ESXi V6.7
Processor	Intel Core i5 (4 cores) with 2.4 GHz or equivalent	Intel Core i7 (8 cores) with 3 GHz or equivalent	2 cores with 2.4 GHz or equivalent	8 cores with 3 GHz or equivalent
RAM	8 GB	8 GB	8 GB	8 GB
Network adapter	1	1 **Note:** SINEMA Server supports up to 16 network adapters.	1 Type: "E1000"	1 Type: "E1000" **Note:** SINEMA Server supports up to 16 network adapters.
Storage requirements hard disk	approx. 10 GB*	approx. 50 GB*	approx. 10 GB*	approx. 50 GB*

* The disk size also includes the capacity presumably required for archive data. When using other programs such as STEP 7, the disk requirements increase accordingly.

Software requirements

Supported operating systems	• Windows 7 SP1 (64-bit) • Windows Server 2016 Standard Version 1607 (LTSB) • Windows 10 (Pro / Enterprise) Version 1803 (64-bit) / 1809 (64-bit)
Supported operating system languages	• German • English • French • Chinese (simplified)

Requirements for the Web client

For users that access SINEMA Server from client systems, the client computer must meet the following requirements:

Web browser	• Internet Explorer 11.0 • Firefox 64.0 or higher • Google Chrome 71.0 or higher • Microsoft Edge 44.0 or higher
Screen resolution for landscape format	
Minimum resolution	1024 x 768 pixels
Recommended, maximum resolution	1920 x 1080 pixels
Screen resolution for portrait format	
Minimum resolution	768 x 1024 pixels
Recommended, maximum resolution	1080 x 1920 pixels

Restrictions and requirements for use with VMware ESXi

When SINEMA Server is used with VMware, the following restrictions and requirements apply:

- SINEMA Server is released under VMware ESXi V6.7.
- PC must be certified for VMware ESXi V6.7.
- Distributed Switch: Not permitted
- Hard disk: Without Thin Provision
- Vmotion and Storage motion: Not supported
- Fault tolerance: Not supported
- DRS and SDRS: Not supported
- Distributed power management: Not supported
- High availability: Not supported

- VMwaretools: Must be installed, automatic update must be disabled.
- Unused hardware should be deactivated.
- Snapshots should not be created when operating SINEMA Server.

User rights

To be able to install SINEMA Server on your computer, you require administrator privileges.

Time required

The time required is estimated to be about 15 to 30 minutes, depending on the computer class and scope of installation. A migration can take up to 2 hours.

Sequence

To install SINEMA Server on your computer, follow the steps below:

1. Log in to the Windows operating system as administrator. Open the Windows Explorer and double-click on the "Setup.exe" file in the root directory of the installation data medium. As an alternative, start the program from the Windows menu **"Start > Run"**.

   If the Auto Run function is enabled for your DVD-ROM drive, the installation will start automatically.

2. Select the language for the Setup wizard of SINEMA Server and click "Next".

   Note

   Setup wizard in the Chinese language

   For the setup wizard only the language Chinese can be used if the installation is made on an operating system with language Chinese (simplified).

3. Click the "Open source license agreement" button to display the license agreement. After reading the license agreement, select the option "I accept the conditions of the above license agreement as well as the conditions of the Open Source license agreement" and then click "Next".
4. Enter the required user information and click the "Next" button.

   A dialog box opens containing the list of programs to be installed. Leave the preselection of the SINEMA Server components as it stands.

   To be able to use SINEMA Server, you also require the Automation License Manager.

   Note

   Requirement for discovery of duplicate IP addresses

   The discovery of duplicate IP addresses is only possible if you also install the "Win10Pcap" component.

5. Select the check box for the Automation License Manager (ALM). If you require further information about the ALM, click the "Readme" button on the right of the dialog box.

6. Select the "Storage space" button to display the current storage space of the computer.
7. Click the "Browse" button if you want to change the standard target directory and install the application somewhere else.
8. Select the required storage location and click the "Next" button to start the installation.

Note

Memory requirements

If the drive does not have enough free storage space, click the "Browse" button to select a different location for the installation.

A new dialog box opens.

9. Follow the further instructions that guide you through the entire installation. This process can take several minutes.

Note

Restart during installation

Depending on the installed .NET version a restart of the PC may be necessary during installation. After the restart, you must log on with the same user with which the installation was started. After logging on the installation continues automatically.

When it is finished, a final window is displayed for the setup. This contains a status message about the successful installation of the SINEMA Server application.

10. In the setup window, you can either restart the computer immediately or later. Select the required option and click the "Finish" button to complete the installation.

2.2.3 Uninstalling SINEMA Server

Uninstalling

To uninstall SINEMA Server from your computer, follow the steps below:

1. Open the Windows Control Panel by clicking **Start > Control Panel** in the Windows taskbar.
2. In the Control Panel window, open the "Add or Remove Programs" dialog box
3. In the sub window of the "Add or Remove Programs" dialog box, click on "Change or Remove Programs".
4. In "Currently installed programs", select the relevant entry.
5. Click the "Remove" button. When prompted to confirm removal, click "Yes". SINEMA Server is then uninstalled from your system.

Note

License key

After uninstalling the program, you can retain the valid license key. To do this, open the Automation License Manager and save the license on a separate data medium. You can also, however, transfer the license to other users.

Note

Closing program files and folders before uninstalling

When uninstalling, the installation program removes the program files and folders. If one of the folders to be uninstalled is still open in the Windows Explorer, an error message is displayed. To avoid this, make sure that the folder to be uninstalled is closed.

2.3 Configuring and starting SINEMA Server

The following section describes what needs to be done to set up and start SINEMA Server on the management station. Before starting SINEMA Server for the first time, basic parameters need to be set that are required for subsequent network access. The SINEMA Server Monitor described below is the central access point for the configuration and starting SINEMA Server as well as for several other services.

2.3.1 SINEMA Server Monitor

Overview

SINEMA Server Monitor is the central program module for administration of SINEMA Server. SINEMA Server Monitor runs on the PC/PG on which SINEMA Server is installed (management station).

SINEMA Server Monitor loads automatically after successful installation of SINEMA Server and on each subsequent Windows startup. In addition to this, the following icon is included in the taskbar for calling up a shortcut menu that provides the functions of SINEMA Server Monitor.

Note: This icon may also be colored differently indicating different statuses of SINEMA Server. You will find the significance of the different colors in the section Status display (Page 30)

Structure of the shortcut menu

Right-click on the icon in the taskbar. Following this, the shortcut menu for calling up the following functions appears:

- "Start web client": The standard browser is opened and SINEMA Server is called with the configured HTTPS port using the URL "https://localhost:<https-port>". If no HTTPS port is configured, SINEMA Server is called using the URL "http://localhost:<http-port>".
- "Start/Stop SINEMA Server": The progress of the action is shown in the "Status" tab of the "Settings" window.
- "Settings": The "SINEMA Server Status" window is opened. This window contains a button for calling the Web client and provides options for making the administration settings for SINEMA Server as described in the following sections. Note the requirement described below for changing settings.
- "Close": SINEMA Server Monitor is exited. You can start SINEMA Server Monitor again with "Start > Programs > Siemens Automation > SINEMA Server > SINEMA Server".

Requirement for editing settings in SINEMA Server Monitor

Settings in SINEMA Server Monitor can only be edited with administrator rights. In SINEMA Server Monitor, click the "Enable administrator mode" button to make the settings of SINEMA Server Monitor editable. If you are logged in as a user with administrator rights, a Windows dialog for user account control appears that you need to confirm. If you are logged in as a user without administrator rights, you need to specify the data of a user that has administrator rights. For the response described it is assumed that at least the second highest level "Standard" was configured for the user account control in Windows. The user account control is available in "Control Panel > User Accounts > User Accounts > User Account Control Settings".

Effect of changes in SINEMA Server Monitor

If you change settings in SINEMA Server Monitor, the Web server is automatically exited and restarted. Open Web sessions with SINEMA Server are interrupted and you need to log in again.

2.3.1.1 Status display

The operational status of SINEMA Server is displayed in the "Status" tab of SINEMA Server Monitor. Using the button of the SINEMA icon and its status text, information about the current system status can be displayed if problems occur. The tab also contains buttons for starting and stopping SINEMA Server.

Meaning of the status displays

The color of the icon indicates the overall status of SINEMA Server. The overall status of SINEMA Server is determined by events from the overall status groups; see section Administration - Events Overall status groups (Page 200).

Icon	Description
	SINEMA Server is stopped or is being started up
	OK
	Maintenance demanded
	Maintenance required

NOTICE

Avoiding shutting down or restarting

Avoid a forced shutdown or a restart while SINEMA Server is in operation. In such situations, it is possible that the SINEMA Server database will be damaged. This means that the application no longer starts up correctly and the only remedy is to reinstall the application.

To avoid loss of data in such situations, it is advisable to back up the system regularly. The backup data can be called up when necessary using the restore function.

Note

Critical system statuses

The system statuses displayed when there is not enough work memory or hard disk space have the following meanings:

- Server hardware: Work memory full, no more memory space available (caution): Work memory ≤ 200 MB
- Server hardware: Hard disk full, no more memory space available (caution) / server hardware: No hard disk space available for archiving (caution): Hard disk space ≤ 300 MB

2.3.1.2 Port settings

With the port settings, you can configure SINEMA Server for HTTP, HTTPS, OPC UA, OPC DA and RPC connections as well as for the use of the SNMP trap port 162. For the individual connection types, the following functions are available:

- HTTP connection (disabled as default):
  - Specify the required HTTP port manually
  - Specify the HTTP port to be used by searching for an available port
  - Enable/disable SINEMA Server for HTTP connections
- HTTPS connections:
  - Specify the required HTTPS port manually
  - Specify the HTTPS port to be used by searching for an available port
  - Enable/disable SINEMA Server for HTTPS connections
  - Generating a new HTTPS certificate, refer to the section "Generating HTTPS certificates"
- OPC DA connections:
  - Enable/disable SINEMA Server for OPC DA connections
- OPC UA connections
  - Specify the required OPC UA port manually
  - Specify the OPC UA port to be used by searching for an available port
  - Enable/disable SINEMA Server for OPC UA connections
- OPC UA server authentication:
  - For access to the OPC UA server specify whether authentication with a user existing in SINEMA Server is necessary. With every user that exists in SINEMA Server, all devices are visible that were included in "Administration > Monitoring > OPC" in the list of devices visible in OPC regardless of the device assignment to views. As default, the setting "With user authentication" is enabled.
- OPC UA security mode:
  Specify which connections are permitted for access to the OPC UA server:
  - None: The OPC UA connections need to be neither signed nor encrypted.
  - Signed / signed and encrypted connections: Only signed connections or signed and encrypted connections are permitted.
  - Signed and encrypted connections: Only connections that are signed and encrypted are permitted.

- RPC connections (to query the overall device statuses of remote servers, Web page "Server overview" - port can also be configured here):
  - Specify the required RPC port manually
  - Specify the RPC port to be used by searching for an available port
- SNMP traps:
  - Windows trap service: If this option is enabled, the Windows trap service is used for shared use of the SNMP trap port 162 with other applications as long as the Windows trap service is enabled in Windows. The Windows trap service needs to be enabled manually to allow SINEMA Server to receive traps with this setting. The Windows trap service is recommended for receiving SNMP traps from NAT devices.
  - SINEMA Server trap service: If this option is enabled, the SNMP trap port 162 is used exclusively by SINEMA Server as long as the Windows trap service is not enabled in Windows.

  Changes to the SNMP trap settings take effect only after restarting SINEMA Server.

Note

HTTP port and HTTPS port

If the HTTP port or HTTPS port is being used by another process, a warning message to this effect appears. This message is marked yellow. In this case, it is advisable to change the port using the "Find free port" option.

To display a list of the processes that use e.g. port 80, you can enter the following command: netstat -noa | findstr :80

Reserved port numbers

SINEMA Server uses the following ports as default ports for communication. Remember, however, that two different programs cannot communicate at the same time via the same port. If, for example, other SIMATIC applications or devices are connected to one of the ports, this port is not available for SINEMA Server.

For this reason, make sure that these ports are available to SINEMA Server when starting up and operating the application. Below, you will find list of the default ports used by SINEMA Server:

Default ports	Description	Corresponding transport protocol	configurable	Note on the response if the port is blocked
22	Secure Shell (SSH)	TCP	yes (Web user interface)	CLI via SSH not possible
23	Telnet	TCP	yes (Web user interface)	CLI via Telnet not possible
25	SMTP	TCP	yes (Web user interface)	-
69	TFTP	UDP	yes (Web user interface)	No firmware download possible

Default ports	Description	Corresponding transport protocol	configurable	Note on the response if the port is blocked
80	HTTP server	TCP	yes (Windows taskbar)	-
102	SIMATIC S7 communication	TCP	no	-
161	SNMP	UDP	yes (Web user interface)	It is not possible to read out device information.
162	SNMP traps	UDP	no	SINEMA Server does not receive any traps.
443	HTTPS	TCP	yes (Windows taskbar)	-
34964, 49152-65535	PROFINET "Read data record"	UDP	no	No PROFINET monitoring possible
4770	RPC port (server-server communication)	TCP	yes *	Device overall statuses cannot be queried.
4841	OPC UA server	TCP	yes (Windows taskbar)	If OPC UA server and OPC UA client are separate PCs, if a port is blocked no OPC UA communication is possible.
4897	Data	TCP	no	SINEMA Server does not start.
4998	Events	TCP	no	SINEMA Server does not start.
4999	Monitor	TCP	no	SINEMA Server does not start.
5432	POSTGRESQL	TCP	no	Saving events / reports is not possible.

* The port number of the old server is configured in the "Port settings" of SINEMA Server Monitor, the port number of the polling server in the Web user interface of SINEMA Server in "Server overview".

As default, the setup of SINEMA Server enters a series of processes in the list of firewall exceptions. Below you will find the processes that are opened by SINEMA Server so that the firewall ports can communicate.

- WCCILpmon.exe - TCP/UDP port
- WCCOAsnmp.exe - TCP/UDP port

NOTICE
Firewall With some firewall configurations, it may be necessary for the system administrator to adapt some of the settings listed above.

Generating HTTPS certificates

As further support for HTTPS connections, the setup of SINEMA Server also includes the generation of HTTPS certificates. As soon as the SINEMA Server setup has been started on a computer, this certificate is generated automatically based on the IP address, the computer name and the FQDN. If the IP address, the computer name or the FQDN is changed, the certificate needs to be regenerated. To generate this certificate again click the "Generate..." button. You can then specify the period of validity of the certificate (1 ... 10 years) and optionally up to 3 additional entries for IP addresses, computer names and FQDNs based on which the HTTPS certificate will be generated.

Using third-party certificates

You will find this certificate in the following folder:

Siemens\SINEMAServer\Sinema_Server\config

- certificate.pem - self-signed certificate
- privkey.pem - private key for the certificate

To obtain a verified certificate, you need to send the self-signed certificate to VeriSign or another trustworthy organization to have it signed. This is necessary if you want to use the certificate later. As an alternative, you can also use a certificate that has already been signed.

In both cases, the newly generated certificate must be stored in the following folder:

- Siemens\SINEMAServer\Sinema_Server\config

NOTICE
SSL certificate The SSL certificate must be stored under the name "certificate.pem".

2.3.1.3 Device profile synchronization

Purpose of device profile synchronization

In networks with more than one SINEMA Server instance, all instances should always use the same device profiles so that the monitored devices are displayed according to uniform patterns. The device profile synchronization function allows a central file path to be specified for new device profiles or device profiles and requiring updates. The stored device profiles are automatically imported into the local SINEMA Server instance at a selectable time of day or at a selectable interval (12 hours / 24 hours). As an alternative, the device profiles stored in the configured file path can be imported manually at any time.

Before performing device profile synchronization, refer to the recommendations in the section Central configuration of device profile data (Page 40).

Compatibility of device profiles from different SINEMA Server versions

The following table specifies the device profiles of which SINEMA Server versions are migrated when you install different SINEMA Server versions.

Device profile originates from version:	Device profile is compatible with version:									
	SINEMA Server V12	SINEMA Server V12 SP1	SINEMA Server V12 SP1 HF1	SINEMA Server V13	SINEMA Server V13 HF2	SINEMA Server V13 SP1	SINEMA Server V13 SP2	SINEMA Server V14	SINEMA Server V14 SP1	SINEMA Server V14 SP2
SINEMA Server V12	-	+	+	!	!	!	!	!	!	!
SINEMA Server V12 SP1	!	-	+	!	!	!	!	!	!	!
SINEMA Server V12 SP1 HF1	!	+	-	!	!	!	!	!	!	!
SINEMA Server V13	!	!	!	-	+	+	!	!	!	!
SINEMA Server V13 HF2	!	!	!	!	-	+	!	!	!	!
SINEMA Server V13 SP1	!	!	!	!	!	-	+	!	!	!
SINEMA Server V13 SP2	!	!	!	!	!	!	-	+	!	!
SINEMA Server V14	!	!	!	!	!	!	!	-	+	!
SINEMA Server V14 SP1	!	!	!	!	!	!	!	!	-	+
SINEMA Server V14 SP2	!	!	!	!	!	!	!	!	!	-

- The SINEMA Server version is not changed

+ Device profile is compatible with version and will be migrated

! Device profile is not compatible with version and will not be migrated

Rules for importing device profiles

When importing existing device profiles, the following rules apply:

- Provided device profiles whose device profile IDs are not available in the local SINEMA Server instance are imported into the local SINEMA Server instance. The import of device profiles is output as an event in the event list.
- Provided device profiles whose device profile IDs exist in the local SINEMA Server instance overwrite the corresponding device profiles in the local SINEMA Server instance. Overwriting device profiles is output as an event in the event list.
- For device profiles in the local SINEMA Server instance whose device profile IDs do not exist in the provided device profiles, the response can be configured as follows:
  - Delete local device profiles without reference to provided device profiles if these local device profiles are not being used as monitoring profiles for existing devices.
  - Retain local device profiles without reference to provided device profiles (default setting).

Note

Avoid multiple device profile archives in the import folder

Make sure that there is only ever one device profile archive in the import folder. If the import folder contains several device profile archives at the same time, these must not have any overlaps with identical device profile IDs.

The table below illustrates the import rules based on examples of device profile imports. The following formatting and naming conventions are used:

- Device profiles formatted in **bold** text in the "Local device profiles" column are used as monitoring profiles for existing devices. Device profiles without this text highlighting are not used as monitoring profiles for existing devices.
- The numbers of the device profiles indicate their device profile IDs.
- The variants indicate differences in content between device profiles with the same device profile ID.

In each of the examples a distinction is made between the "Delete local device profiles without assignments" option being enabled and disabled.

Local device profiles	Provided device profiles	Local device profiles after profile import	
		"Delete local device profiles without assignments" option is enabled	"Delete local device profiles without assignments" option is disabled
• Device profile 1, variant a • Device profile 2, variant a • **Device profile 3, variant a** • **Device profile 4, variant a**	• Device profile 1, variant a • Device profile 3, variant a	• Device profile 1, variant a • Device profile 3, variant a • Device profile 4, variant a	• Device profile 1, variant a • Device profile 2, variant a • Device profile 3, variant a • Device profile 4, variant a
• Device profile 1, variant a • **Device profile 3, variant a**	• Device profile 1, variant a • Device profile 2, variant a • Device profile 3, variant a • Device profile 4, variant a	• Device profile 1, variant a • Device profile 2, variant a • Device profile 3, variant a • Device profile 4, variant a	• Device profile 1, variant a • Device profile 2, variant a • Device profile 3, variant a • Device profile 4, variant a
• Device profile 1, variant a • Device profile 2, variant a • **Device profile 3, variant a** • **Device profile 4, variant a**	• Device profile 1, variant b • Device profile 3, variant b	• Device profile 1, variant b • Device profile 3, variant b • Device profile 4, variant a	• Device profile 1, variant b • Device profile 2, variant a • Device profile 3, variant b • Device profile 4, variant a
• Device profile 1, variant a • **Device profile 3, variant a**	• Device profile 1, variant b • Device profile 2, variant b • Device profile 3, variant b • Device profile 4, variant b	• Device profile 1, variant b • Device profile 2, variant b • Device profile 3, variant b • Device profile 4, variant b	• Device profile 1, variant b • Device profile 2, variant b • Device profile 3, variant b • Device profile 4, variant b

Configuring device profile synchronization

Device profile synchronization can be configured in SINEMA Server Monitor as follows:

Operator control element	Function
Scan	Select the folder in which the device profiles to be imported will be stored.
Options	Specifying user data for access to profile update directory.
Automatic synchronization	If this check box is enabled, device profiles stored in the selected file path are imported automatically into the local SINEMA Server instance. With the "Start time" input boxes, you can configure the time at which the next automatic update is performed. With the two option buttons "12 hours" or "24 hours", the interval for the later automatic updates can be specified.
Delete local device profiles without assignments	• Check box is enabled: Device profiles of the local SINEMA Server instance whose device profile IDs do not exist in the provided device profiles are deleted in the local SINEMA Server instance during import if these device profiles are not used as monitoring profiles for existing devices. Deleting an existing device profile is output as an event in the event list. Note: If this check box is enabled, no import should be performed while the device profiles are being put together in the selected directory. Otherwise, this can lead to the unwanted loss of local device profiles. • Check box is disabled (default): Device profiles of the local SINEMA Server instance whose device profile IDs do not exist in the provided device profiles, are retained when importing into the local SINEMA Server instance.
Import manually	Manual import of the device profiles.

2.3.1.4 Restoring system backups and forcing process aborts

Restoring system backups

Using the "Transfer back" button, a system backup created with the corresponding job can be selected and restored manually. If SINEMA Server cannot be started correctly, the last created system backup is transferred back automatically. The path on which SINEMA Server searches for this system backup can be configured in the job type-specific settings, refer to the section Job type-specific settings for the job type "System backup" (Page 229).

It is possible to restore system backups that were created on a different management station. System backups of SINEMA Server versions V14 SP1 and V14 SP2 can be restored. To restore system backups of the SINEMA Server version V14 in SINEMA Server V14 SP2, the system backups must first be restored in SINEMA Server V14 SP1.

Note

Increased memory requirements during the restoration of system backups

During the restoration of a system backup, due to the intermediate storage of the data in temporary directories, there is an increase in the memory requirements.

Forcing process aborts

The use of the function "Force SINEMA Server to close" can be useful if SINEMA Server cannot be terminated with the "Stop SINEMA Server" button. A loss of data might, however; occur.

When using the function “Force stoppage of creation / transfer back of system backups” system backups being created are discarded and the transfer back of system backups is stopped. Until a system backup has been restored completely, SINEMA Server cannot be started.

2.3.2 Central configuration of device profile data

All device profiles as well as overall status groups and events should be administered in a central SINEMA Server instance and then distributed to the other SINEMA Server instances using device profile synchronization or manual export / import. Device profiles provided by Siemens should first be imported into the central SINEMA Server instance and then synchronized with other SINEMA Server instances. If device profiles on multiple SINEMA Server instances are extended by user-defined overall status groups and events, this can lead to unwanted overwriting of data when exchanging device profiles with other SINEMA Server instances.

2.3.3 Start SINEMA Server

Automatic start

SINEMA Server is started automatically after installation and each time the management station is restarted.

Manual start

If SINEMA Server was exited, you can start the application manually as follows:

- "Start SINEMA Server" menu command in the shortcut menu of the SINEMA Server icon displayed in the taskbar
- "Start SINEMA Server" button in the "Status" tab of the "SINEMA Server status" window

NOTICE
Avoid pauses or idle times on the management station Make sure that the management station does not change to the pause or idle status. This leads to unpredictable reactions relating to device status calculations and reachability. If such a situation does occur, the application needs to be restarted.

2.4 Migrating a SINEMA Server configuration

2.4.1 Migrating a SINEMA Server V14 SP1 configuration to SINEMA Server V14 SP2

Migrating a SINEMA Server configuration allows the adoption of the existing database.

Migration to SINEMA Server V14 SP2 is only possible for configurations originating from SINEMA Server V14 SP1. Older configurations must first be migrated to SINEMA Server V14 SP1.

Before and after each step in migration a system backup should be created. Restoring system backups in SINEMA Server V14 SP2 is not possible for configurations that originate from an older version than SINEMA Server V14 SP1. These system backups must first be restored in SINEMA Server V14 SP1.

The migration is performed as follows:

- Prior to migration SINEMA Server must be stopped via SINEMA Server Monitor.
- After starting the installation routine, SINEMA Server proposes the adoption of the existing database.

SINEMA Server is released for VMWare ESXi V6.7. If SINEMA Server is to be used with VMWare ESXi, VMWare ESXi must be upgraded to VMWare ESXi V6.7.

As of SINEMA Server V14 SP2, PROFINET monitoring is disabled by default. If devices are to be monitored with PROFINET after migration, PROFINET monitoring must be enabled under "Administration > Monitoring > General".

In SINEMA Server V14 SP2, the settings for configuring time spans in the prefilter settings for events have been adapted. If you used the "One month" prefilter setting in SINEMA Server V14 SP1, you must manually enter the corresponding period in the "User-defined" prefilter setting after the migration.

As of SINEMA Server V14 SP2, the monitoring setting "Consider duplicate PROFINET device names in topology" is available and enabled by default. If no PROFINET device names are assigned twice in your network, you can disable this setting after the migration under "Administration > Monitoring > General".

2.5 Web user interface

2.5.1 Logging in to the Web interface of SINEMA Server

Using the Web browser or the options of SINEMA Server Monitor, you can log in to the Web interface of SINEMA Server as follows:

- On a client computer

  You use a Web browser.

- On the management station
  - You use a Web browser specifying the address "localhost".

  or

  - You use the "Start Web client" function of SINEMA Server Monitor

---

Note

Using the HTTPS protocol

For security reasons, it is strongly recommended that you use the HTTPS protocol. The data is transferred encrypted and cannot be read by unauthorized third persons.

Note

Accepting cookies

To be able to work with SINEMA Server, the Web browser used must accept cookies.

Note

Setting the security level for access zone in Windows

For the zone in which SINEMA Server is accessed in "Control Panel > Network and Internet > Internet Options > Security" the security level "Medium-High" may be set as maximum. With the security level "High" it is not possible to log on to SINEMA Server.

NOTICE

"Start Web client" function of SINEMA Server Monitor - default Web browser

When the Web client is called, the SINEMA Server Monitor uses the Web browser set as default in Windows. SINEMA Server supports the Web browsers listed in the section Installing SINEMA Server - requirements and procedure (Page 25). It is advisable to make sure that one of these Web browsers is configured as the default browser.

Logging in on a client computer

To log in to the Web interface of SINEMA Server on a client computer, follow the steps below:

1. Open the Web browser.
2. Enter the IP address of the management station. In the address bar of the browser, enter **http://<**IP address**>** or **https://<**IP address**>** (if the data is to be transferred encrypted).

   If you use a port other than 80 as the HTTP standard port, enter the port number along with the IP address. A colon ":" must be entered between the IP address and the port number as a delimiter (e.g.: http://192.168.0.1:8080). This applies analogously to the HTTPS standard port 443.
3. Enter the user name and the password in the displayed login dialog. By default, this login dialog is displayed in the language that is set in the Web browser used. You can change the language of the SINEMA Server web user interface with the  button as well as after you have logged on to the SINEMA Server.

   If authentication is successful, you will have access to the SINEMA Server Web interface.

Logging in on the management station

To log in to the Web interface of SINEMA Server on the management station, follow the steps below:

1. Open the Web browser.
2. In the address bar of the browser, enter **http://<localhost>** or **https://<localhost>** (if the data is to be transferred encrypted).

   If you use a port other than 80 as the HTTP standard port, enter the port number along with the IP address. A colon ":" must be entered between the IP address and the port number as a delimiter (e.g.: http://192.168.0.1:8080). This applies analogously to the HTTPS standard port 443.
3. Enter the user name and the password in the displayed login dialog. By default, this login dialog is displayed in the language that is set in the Web browser used. You can change the language of the SINEMA Server web user interface with the  button as well as after you have logged on to the SINEMA Server.

   If authentication is successful, you will have access to the SINEMA Server Web interface.

or

1. Select the "Start Web client" function in SINEMA Server Monitor.
2. Enter the user name and the password in the displayed login dialog. By default, this login dialog is displayed in the language that is set in the Web browser used. You can change the language of the SINEMA Server web user interface with the  button as well as after you have logged on to the SINEMA Server.

   If authentication is successful, you will have access to the SINEMA Server Web interface.

Note

Recommendation: Use a secure port or HTTPS

When you log in to the Web interface of SINEMA Server, you should ideally use the HTTPS protocol.

NOTICE

Avoiding shutting down or restarting

Avoid a forced shutdown or a restart while SINEMA Server is in operation. In such situations, it is possible that the SINEMA Server database will be damaged. A damaged database means that the application no longer starts up correctly and the only remedy is to reinstall the application.

To avoid loss of data in such situations, it is advisable to back up the system regularly. The backup data can then be called up when necessary using the restore function.

Initial credentials

As default, the predefined user "Administrator" is available in SINEMA Server. This user is assigned to the predefined user group of the same name. The default user name and the password for this user are as follows:

- User name: Administrator
- Password: SinemaA

After the first logon to the system, you will be prompted to change the initial password in "Administration > My settings". When the new password is entered, its password strength is checked. You can find more information in the section Password strength (Page 238).

Note the mechanisms for protection against brute force attacks, refer to the section Administration - User Logon locks (Page 212)

If you have forgotten your password you can have a one-time password sent to you using the "Forgotten the password?" button. This one-time password is then sent to the e-mail address stored for the user.

Note

Configuring e-mail settings for administrators

At least for users with administrator rights, configure the e-mail settings so that when necessary you can be sent one-time passwords.

You will find further information about these predefined user groups, access rights and creating/managing users in the section Users and user groups (Page 66)

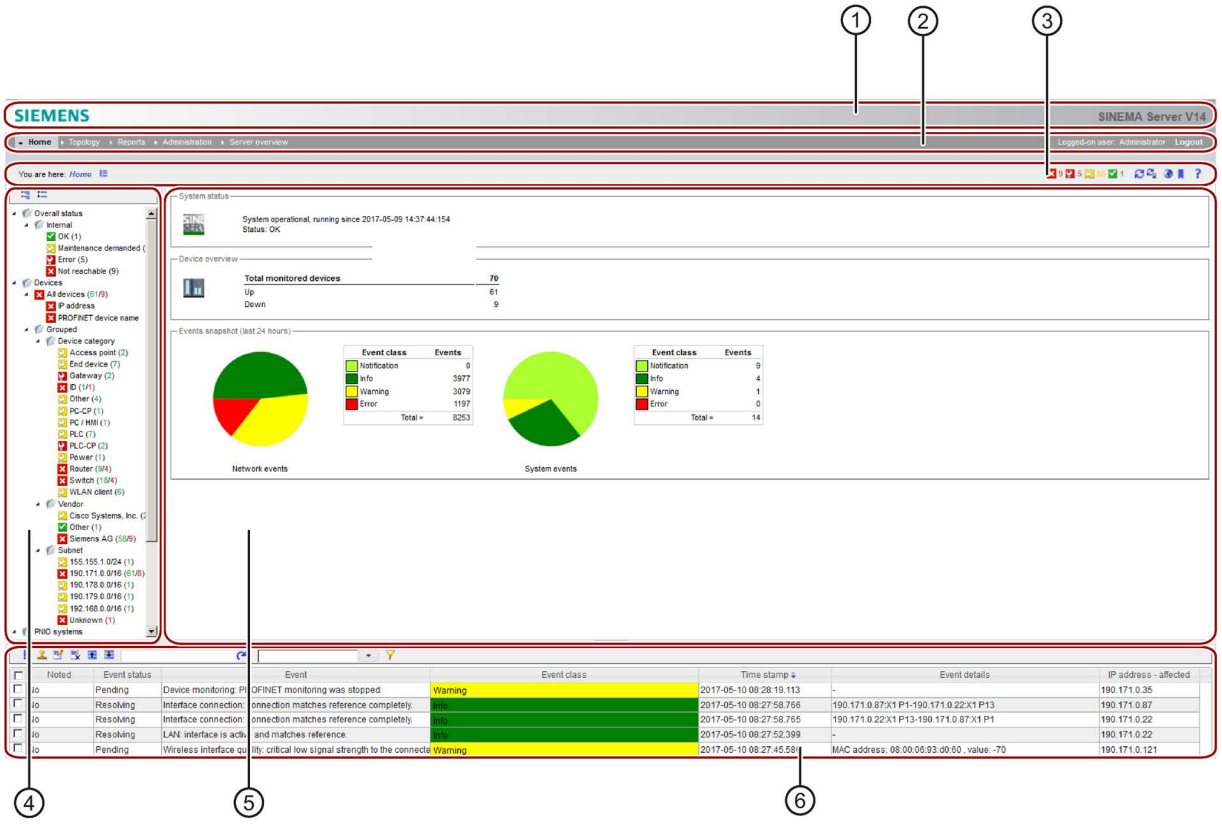
The most important action before first using the application is to scan the devices in the network. For more detailed information, refer to section Detecting devices in the network (Page 49)

2.5.2 SINEMA Server user interface on the Web interface

Program window

The program window of SINEMA Server is divided into several areas, some of which are always visible and always have the same type of content. These areas contain both general information and operator controls for performing basic program actions.

The following screenshot shows the program window with its permanent areas and the main window for the specific views.



① Header area
② Navigation bar
③ Status bar
④ Device tree
⑤ Main window
⑥ Event list

Operation / content

The individual areas of the program window are explained below in detail with their information content and the functional options.

- **① Header area**

  This area contains the SIEMENS logo and program name (SINEMA Server V14).

  Note

  Displaying program information

  If you click on the program name, an information window opens. It contains program information such as version number, release date and extent of the license.

- **② Navigation bar**
  - 1st row:

    To the left in the navigation bar is the first level of the menus, from which you can call the individual program functions. The right area displays your username and the logout button. For reasons of security, always click this button when you want to end your work with SINEMA Server. Closing browser windows and browser tabs without logging out first should be avoided for security reasons.

    The content of the menu bar varies depending on the status of SINEMA Server. The "Topology" and "Reports" menu items are displayed only following an initial discovery.
  - 2nd row:

    This shows the menu commands of the second level, depending on the command you have chosen in the first level.

    On the right, information texts are displayed indicating certain actions or operational statuses.

- **③ Status bar**

  In the left area, you see the branch of the menu tree you are in, and also the part of the program or the window that is currently open.

  The right-hand section of the status bar contains the following function elements:

Icon	Display / function	Icon	Display / function
	Full screen mode on/off (hide/show the device tree and events)		(animated): A search is made for more suitable device profiles and device types included in them for devices that were assigned standard profiles.
	(with number): Number of unreachable devices Opens the device list with the display of the unreachable devices. The number of devices involved is displayed.		(animated): Network is scanned
	Opens the device list with the display of the devices with the status "Maintenance demanded". The number of devices involved is displayed.		Opens the device list with the display of the devices with the status "Error". The number of devices involved is displayed.
	Opens the device list with the display of the devices with the status "OK". The number of devices involved is displayed.		Opens the device list with the display of the devices with the status "Maintenance required". The number of devices involved is displayed.
	Opens the device list with the display of the devices with the status "not connected". The number of devices involved is displayed.		Autorefresh on/off The content of the Web page is refreshed according to the interval configured in "Administration > My settings > User interface".
	Refresh display SINEMA Server refreshes the content of the Web page once.		Managing and using quick links Opens the list of available quick links.
	Select language A selection dialog with the available languages is displayed. The changeover also affects the display of the online help.		Printing The print function is available on the following Web pages: • Topology • Reports

Icon	Display / function	Icon	Display / function
	Open help system Opens the help page for the current Web page in a separate window of the Web browser.		

- **④ Device tree and views**

  The device tree contains groups of devices that are monitored by the local SINEMA Server instance or by other SINEMA Server instances. Selecting a device group below the "Overall status > Local" and "Devices" branches generates a display filtered according to the overall status or device property (device category, vendor, subnet, alternating devices). Selecting an entry below the "Server overview" branch results in a display of the server overview sorted according to overall device statuses. After selecting a node under the entry "PNIO systems", only the devices that belong to the selected PNIO system are displayed. The icons in the device tree always show the worst current status of one of the device nodes in the branch.

  Views are used to monitor any subareas of a network based on lists and topology displays. By assigning views to individual users, the network areas to be monitored can be restricted to specific users.

- **⑤ Main window**

  Depending on the selected function, the main window contains the generated display.

- **⑥ Event list**

  The event list shows network events that have occurred as well as system-related events. Initially, the display is sorted chronologically. By clicking on the relevant column headers, you can sort the display according to any property in ascending or descending order. Other operating options are provided by the toolbar located above.

Selecting the language of the user interface

You can change the language of the Web user interface at any time "online" by clicking the corresponding icon in the header. The changeover also affects the display of the online help.

Updating the Web user interface

The content of the Web user interface is updated either cyclically or on demand.

This is selected using the relevant icons in the status bar.

You set the interval for cyclic operation with the menu command "Administration > My settings > User interface" in the "Monitoring interval" parameter.

Getting to know SINEMA Server - basic functions 3

3.1 Detecting devices in the network

3.1.1 Overview

The basic requirement for setting up network monitoring in SINEMA Server is the network scan for device discovery. You initiate this activity after starting SINEMA Server for the first time and, when necessary, at the touch of a button or automatically in suitably configured cycles.

When scanning devices in the network, the following is started in SINEMA Server:

- During the first scan, reachable devices are searched for based on selectable protocols.

  Depending on the configuration in SINEMA Server, either all the devices discovered by DCP and/or ICMP or devices in preset address ranges are recorded.
- The devices discovered using ICMP and optionally DCP are displayed in the device list. Information about the interfaces of the discovered devices is displayed in the interface list. The discovered connections are displayed in the topology display.
- If SIMATIC controllers are found during the scan, the IO devices assigned to these controllers can also be included in the monitoring. This is the case regardless of whether the IO devices are located in the scan range or not.
- Based on the discovery rules in the profile data, the devices are assigned to a suitable device profile. Devices that cannot be assigned to any discovery rules are assigned to default profiles, if these default profiles are enabled. If the default profiles suitable for devices are not activated, these devices are not assigned to a device profile and the devices are not monitored, see also the heading "Limited device detection by disabling default profiles" in the section Device discovery in the network (Page 50). If the PROFINET discovery is active for a device profile, devices can be assigned to this device profile and the device types it contains using article numbers.
- The detected devices are changed to the "Monitored device" status in SINEMA Server. (Note: the number of devices in the "Monitored" status is limited by the SINEMA Server licensing.)
- When you scan again, newly added devices are detected. The device list, the interface list and the topology display are then updated. Removed devices are no longer shown in the device and interface list or in the topology display.

3.1.2 Device discovery in the network

Requirements - adapting the scan range

Before you start the scan for the first time, it is advisable to adapt the scan range.

If you do not adapt the scan range, the device scan can take a very long time if there is a very large scan range. If the scan range covers more than 1000 addresses, a message will warn you to expect the scan to take a long time. You should therefore generally restrict the scan range to the devices to be monitored. To do this, it is advisable to create smaller scan groups if the IP addresses are not consecutive. This division speeds up scanning of the devices. A maximum of 100 scan groups can be created.

By default, SINEMA Server calculates the start and end of the scan range based on the IP address and subnet mask configured on the network interface adapter.

The procedure described below includes the adaptation of the scan range.

Network scan - procedure

To scan the network, follow the steps below:

1. Select the menu command **"Administration > Discovery"**, "Scan" tab.
2. In the section "DCP network adapter for device scan", select the function "Scan for network adapters".

   The network adapters available on the management station are displayed.
3. In the table, select the network adapters (called NIC below) over which the scan will run and enable these using the "Enable network card for device scan" function.
4. When necessary, enter further parameters in the following Web pages:
   - "Administration > Discovery" in the "Profiles" tab
   - "Administration > Monitoring > General" in the "Time settings" area
   - "Administration > Monitoring > SNMP settings"
5. If applicable, select the menu command **"Administration > Discovery"** again and open the "Scan" tab.
6. Select the IP address ranges to be searched.
7. Click on the "Start scan" icon to start the network scan. The network is scanned according to the scan ranges for the subnets.

- The progress of the scan is indicated by an icon in the right part of the status bar.
- On completion of the scan, all discovered network devices and their statuses are displayed in the device lists that can be selected in the device tree.

Limited device detection by disabling default profiles

SINEMA Server only monitors devices that have been assigned to device profiles. If SINEMA Server does not find a suitable profile for a device, it assigns a default profile to the device to ensure that it is monitored. To deliberately exclude devices from monitoring, device profiles can be disabled under "Administration > Discovery > Profiles". This is also possible for default profiles.

Disabling the default profiles can have the following consequences:

- Devices that cannot be assigned to a profile (device-specific profile or default profile) are not entered in SINEMA Server and are therefore not monitored by SINEMA Server. This can occur especially with devices from third-party manufacturers for which no device-specific profiles have been created.
- The topology display is incomplete because not all devices found were entered in SINEMA Server.
- PNIO systems may be incomplete due to missing devices.
- During the network scan, SINEMA Server detects the devices in the first step and assigns them to device profiles in the second step. Devices that were recognized are already displayed in SINEMA Server after the first step. Devices that cannot be assigned to any profiles are hidden again after the search.

A list of all devices - both those entered in SINEMA Server and those not entered - is specified in a log file "scanresult_log_[time stamp].csv" in the directory "\Siemens\SINEMAServer\DiscoveryLog".

Special features to note

Note

Effect of the option "Include all devices discovered with DCP in the result"

If you select the option "Include all devices discovered with DCP in the result" in the DCP scan settings, note the following:

With this setting, it is possible that DCP devices that are outside the IP ranges but within the subnets connected to the NICs are also detected.

NOTICE

Avoid stopping/starting during the network scan

If SINEMA Server is stopped during the scan and then restarted, this can lead to inconsistent responses in the application. As result of this, it is possible that the discovered network devices do not change to the monitored status. The information under "Device details" and "Device topology" may also not be available. To avoid this, keep to the following rules during scanning:

- Before stopping SINEMA Server, make sure that the scan has not started.
- If devices were found during an aborted scan, delete these and scan the network again.

NOTICE

Do not change the date or time

While the SINEMA Server application is running, it is advisable not to change the date or time of the system in any way. Such changes impact on the application and cause unwanted secondary effects.

Note

Updating device data already read in

Read device data is updated cyclically. You can perform the update manually with the "Update user interface" button.

3.2 Monitoring devices with network topologies

3.2.1 Topology - Overview

SINEMA Server provides the option of monitoring devices using network topologies. Network topologies visualize network connections between the devices and provide detailed information on devices and connections.

To obtain the topology information SINEMA Server uses the protocols SNMP and/or PROFINET. Due to the information made available to SINEMA Server by the devices to be monitored, the detected network status an deviate from the real network status.

Editing mode

In the Editing mode based on the topology detected by SINEMA Server, you can configure a reference topology representing the expected status of the network. With the aid of a connection wizard you can configure reference connections and specify reference statuses for device ports. The configured reference topology forms the basis for monitoring the network in the Online mode and in view-specific topology displays.

Online mode

In Online mode you can monitor the devices and the current network topology taking into account the configured reference topology. Deviations between detected statuses and configured statuses are highlighted optically by SINEMA Server.

3.2.2 Configuring the reference topology in the Editing mode

Meaning

After you have configured the reference topology in the Editing mode, you can monitor the network in the Online mode and in view-specific topology displays taking into account your presettings.

Procedure

1. Select the "Topology" menu command.
   If no reference topology is yet available, and you have the right "operative monitoring settings", the topology is displayed in the Editing mode. You can recognize this by the icon .
2. If all the statuses for devices, ports and connections detected by SINEMA Server are to be adopted in the reference topology, click the icon .
   If the detected information differs from the desired reference status, follow the steps below:
   - Devices A device that is not part of the reference topology is displayed with a star symbol. To define such a device as a reference device, right-click on the device and select the "Adopt in reference topology" menu command. To remove a device from the topology display, select the menu command "Delete".
   - Ports: Select the device for whose ports you want to specify reference statuses. In the "Port overview" area in the right side bar, right-click on a port and select the required reference status. This is only possible for reference devices.
   - Connections: From the toolbar select the drawing tool and then click on the two devices between which the connection will be drawn. Then in the Connection wizard select the ports of these devices involved with the connection. To adopt a single discovered connection as a reference connection, right click on the connection and select the menu command "Adopt in reference topology".
3. Click on the icon to save the configured reference topology and click the icon to change to the Online mode.

See also

Topology (Page 134)

3.3 Setting up network devices individually - using the Profile editor

3.3.1 Profile concept

Profiles give SINEMA Server flexibility during device discovery, device monitoring and device display. Profiles describe device types in terms of common properties.

SINEMA Server distinguishes the following types of profile:

- General profile

  This profile type contains information required for discovery and monitoring of a network device.
- Monitoring profile

  This profile type contains information that is only required for monitoring a network device.

Based on the stored profiles, when each device is detected the first time, SINEMA Server searches for the profiles containing suitable discovery rules. The assigned profile is used to classify and represent the network device. Only devices to which profiles have been assigned can be monitored by SINEMA Server. If no suitable profile is found for a network device during the network scan, SINEMA Server assigns a standard profile to the device. To intentionally exclude devices from monitoring by SINEMA Server, you can disable the default profiles. Read the notes under the heading "Limited device detection by disabling default profiles" in the section Device discovery in the network (Page 50).

Create new profiles

New profiles are always created based on existing profiles. To create a new profile, you must therefore always use an existing profile as the template.

To assign a profile to device types that do not correspond to any previously stored profile, you have the following alternatives:

- You assign the new device type to an existing profile.
- You create a new profile and store the new device type in it.

The assignment of devices to the new device type can then also be performed with the automatic reassignment of profiles; refer to the section below.

Default profiles

If no assignment based on the discovery rules of profiles is possible during the discovery of a device, SINEMA Server assigns an enabled default profile to this device that has not been uniquely identified. You cannot assign devices to disabled profiles.

- Step 1:

  If it is clear from the device ID that this is a Siemens device, one of the following enabled default profiles is used:

  – SIEMENS_Standard

  – SIEMENS_Basic

- Step 2:

  If no assignment is possible in step 1, an enabled default profile is assigned based on the protocols supported by the device.

  – DEFAULT_SNMP_DCP_Device

  – DEFAULT_SNMP_Device

  – DEFAULT_DCP_Device

  – DEFAULT_ICMP_Device

Device discovery using SNMP

During discovery, SINEMA Server attempts to identify the following criteria based on the SNMP data of the device:

1. sysDescr (OID 1.3.6.1.2.1.1.1.0):

   A textual description of the device (system hardware type, software operating system, network software etc.).

2. lldpLocSysDesc (OID 1.0.8802.1.1.2.1.3.4.0):

   The value of the character string is required for the system description mentioned above. If the local agent supports IETF RFC 3418, the lldpLocSysDesc object should have the same value as the sysDescr object.

3. automationSwRevision (OID 1.3.6.1.4.1.4329.6.3.2.1.1.5.0)
4. automationOrderNumber (OID 1.3.6.1.4.1.4329.6.3.2.1.1.2.0)
5. DiagMonitor_StationOrderNumber (OID 1.3.6.1.4.1.4196.1.2.2.13.0)

   Article numbers of SIMATIC IPCs on which the software "DiagMonitor" was installed (only for SIMATIC IPC device profiles)

6. DCP_ID
7. sysObjectID (OID 1.3.6.1.2.1.1.2.0):

   This value is assigned within the "SMI enterprises sub tree" (1.3.6.1.4.1) and contains the highest OID under which the private MIB of the device manufacturer can be found.

Automatic profile and device assignment

Based on the SNMP data, for each newly discovered device, SINEMA Server searches for the profiles containing the suitable discovery rules.

- Step 1 - deciding on the profile

  If more than one profile has a rule that suits the device, the priority of the rule decides which is used.

  If the same criterion exists in more than one profile, the profile with the criterion whose stored text is longest wins.

- Step 2 - using device type rules for the device within the selected profile

  SINEMA Server identifies the suitable device type and uses the icon specified here for the display. If the device type cannot be identified, SINEMA Server uses the default symbol stored in the profile.

Device discovery using PROFINET

The PROFINET discovery can be enabled in the "Basic data" tab of a device profile. This activates device profile and device type rules for this device profile that contain the article numbers of the devices identifiable via PROFINET as assignment criteria. After enabling the check box in the "Criteria" area, the article numbers of device type rules can be edited. The corresponding device profile and device type rules are then updated automatically.

Automatic reassignment of profiles and device types

For devices that were assigned one of the standard profiles during discovery, SINEMA Server runs through the process described above for automatic profile and device type assignment again at regular intervals looking for more suitable profiles and device types they contain for these devices. The default interval for automatic reassignment is 70 minutes and this can be configured in "Administration" > "Monitoring" in the "Time settings" area. In addition to this, the automatic reassignment is always performed when a device with an assigned standard profile changes from the "Not reachable" status to the "Reachable" status.

Note

Effect of assignment of the reference topology

If a device has been assigned a new device profile, it is automatically removed from the reference topology and must be adopted again as a reference device.

3.3.2 Setting up profiles and assigning device types

The following actions are described below:

- Add a new device type to an existing profile
- Create a new profile

Adding a new device type to an existing profile - procedure

To add a new device type to an existing profile, follow the steps below:

1. Open the "Profiles" tab with the **"Administration > Discovery"** menu command
2. Select the profile and open it with the "Edit" button or double-click on the list entry.
3. Change to the "Discovery rules" tab

   Device type rules are taken into account only after evaluation of the discovery rules of the device profile. For this reason, at least one discovery rule must exist that matches the device type to be added.
4. Change to the "Device types" tab and select the "Add device type rule" function

   The Device type editor opens and you can enter the data for the new device type rule.
5. Follow the steps below in the Device type editor:
   - Enter the name of the rule in the "Name" box. This is only the name of the rule not the name of the new device type.
   - Enter the name of the new device type in the "Device type" box.
   - Select the icon of the new device type.
   - Specify the criteria for assigning devices to the new device type, see section The Profile editor (Page 179)

Creating a new profile -principle

When creating a new profile, you always base this on an existing profile. For this reason in the first step, you check which of the existing profiles represents the most suitable basis.

If you intend to create a new general profile, it is advisable to use an existing default profile as the basis.

The following default profiles are available:

- Standard SNMP with DCP approval (name: DEFAULT_SNMP_DCP_Device)
- Standard SNMP (name: DEFAULT_SNMP_Device)
- Standard DCP (name: DEFAULT_DCP_Device)
- Standard ICMP (name: DEFAULT_ICMP_Device)

To be able to select the suitable profile, you should know the protocols used in the new device family.

Creating a new profile - procedure

To create a new profile, follow the steps outlined below:

1. Open the "Profiles" tab with the **"Administration > Discovery"** menu command
2. Select the default profile and select the "Create profile" function.

   This opens the "Add profile ID" dialog.
3. Now assign a unique profile ID. This is used globally in SINEMA Server as the profile ID.

   As an option, decide whether or not the properties of the basic profile you are using should be copied:

   – Discovery rules

   – Device type rules
4. Confirm your entry.

   The Profile editor opens and you can enter the data for the new profile.

Follow the steps below in the Profile editor:

1. Enter the name of the profile in the "Basic data" tab. Select the other parameters including the required default icon for the profile.
2. Change to the "Discovery rules" tab and enter one or more rules required for the discovery of a device of this profile.
3. Change to the "Device types" tab to specify device types individually within the profile and to assign the device type rule.

Creating a monitoring profile - principle

The procedure corresponds to the steps described earlier in "Creating a new profile". The "Discovery rules" and "Device types" tabs are omitted here.

To create a monitoring profile for a specific device in addition to a general profile, use the corresponding general profile as the base profile for creating the new monitoring profile.

You then assign this monitoring profile to the device. This separates the profiles required for device discovery and for device monitoring.

See also

Administration - Discovery / Profiles (Page 177)

3.4 Configuring event reactions - displaying events

Events are divided into the following categories:

- Network events

  Network events provide information about statuses arising and changes in the network. These also include SNMP traps and SIMATIC event and alarm messages sent to SINEMA Server by devices managed in the network.

- System events

  System events provide information about actions, changes and error events of SINEMA Server.

Events of both categories are also divided into the following classes according to their severity:

- Notification and information:

  Events of these classes are generally messages/updates relating to the network and network devices. In contrast, at the system level, these events are generated as result of changes in the performance of SINEMA Server.

  Notifications and information require no action from the end user. These involve either a message about a user action performed by the application or an update due to status changes of network devices. Among others, examples are: User logins/logouts, completion of device discovery, checking of software drivers, start/end of the network scan or permissions granted by the administrator.

- Warning:

  A warning indicates a status that could cause a problem in the future. After receiving the warning message, some action is necessary to ensure the problem-free operation of the devices in the network. These actions then prevent future errors/faults or traps on network devices or in the SINEMA Server application.

  Examples of events of the "Warning" class include:

  – Trap(s) received
  – Start of a device reply to DCP
  – Link down received, link up received
  – Connections activated/deactivated

- Errors:

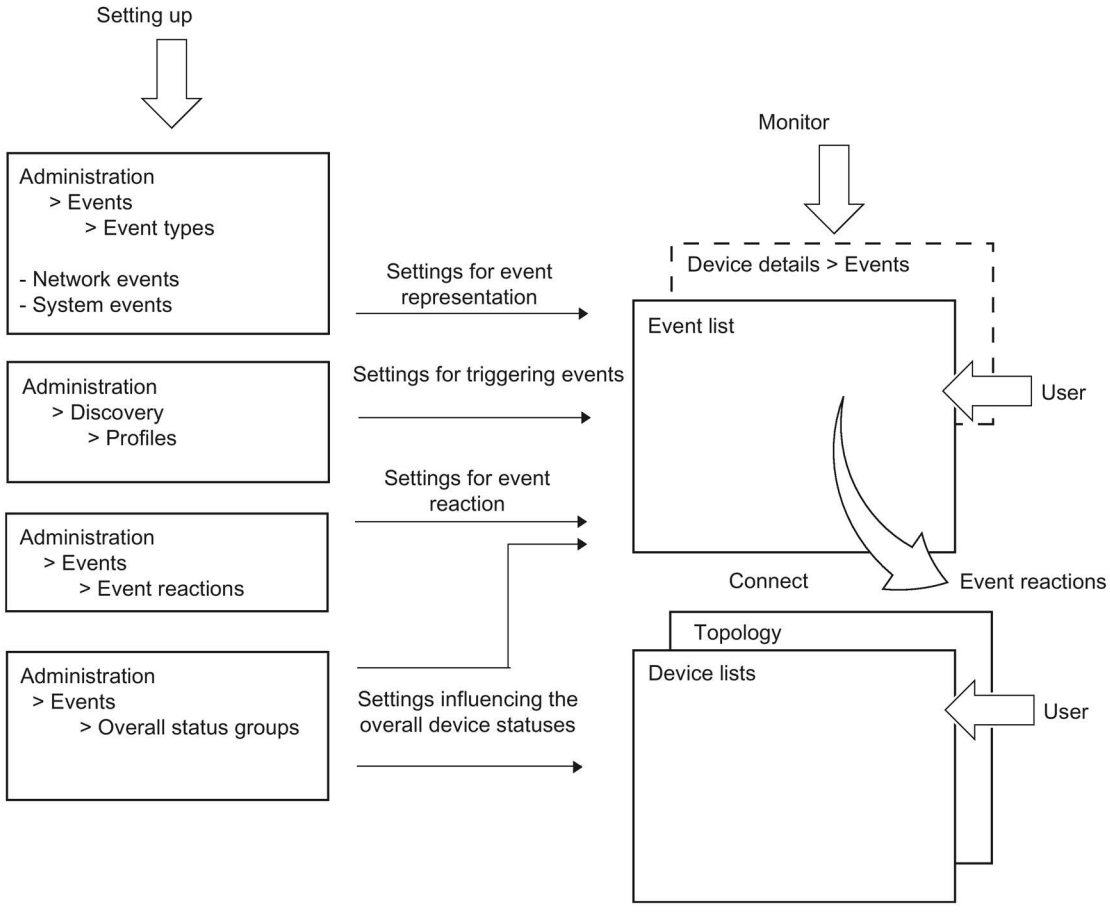
  When such events occur, fast intervention is required. Depending on the content of the error message, the user must take suitable measures. The event reactions already configured for the error events simplify things.

  Examples of events of the "Error" class include:

  – DCP subtask is not executed
  – Scan manager is not run
  – Memory assignment failed
  – Callback address invalid

Setting up and monitoring events in SINEMA Server

The following graphic illustrates the relationships of the SINEMA Server functions for setting up and monitoring network and system events.



- Setting up events

  Setting up the events is part of administration.

  – Settings for the event display

    You make the settings for the event display with the **"Administration > Events > Event types"** menu command.

    Here, you specify new event types and select the event types to be actively monitored. You can also adapt existing event texts and classifications.

    You will find more detailed information on this function in the section Administration - Events Event types (Page 198)

  – Settings for triggering events

    You make the settings for triggering events with the menu command **"Administration > Discovery > Profiles"**.

    In the "Threshold" tab of the profile properties of a device profile, you can use operators and threshold values to define conditions for certain event types in which the corresponding events will be triggered. These conditions then apply to all devices to which the device profile is assigned.

    User-defined network events cannot be triggered without the assignment to a threshold.

    Some of the predefined events can also be triggered even without a link to a threshold.

    You will find more detailed information on this function in the section The Profile editor (Page 179)

  – Settings for the event reaction

    You make the settings for the event reaction with the menu command **"Administration > Events > Event reactions"**.

    Here, you specify the reactions to events or status changes. You can also specify the context to which the reaction should relate. You can choose between the views, device and system.

    By selecting a SINEMA Server view, you achieve the situation that the defined reaction will take place when the device affected by the event is part of the selected view. This allows you to define a view-specific event reaction.

    You will find more detailed information on this function in the section Administration - Events > Event reactions (Page 205)

  – Settings influencing the overall device statuses

    You make the settings for the influence of events on the overall statuses with the menu command **"Administration > Events > Overall status groups"**.

    An overall status group is a group of functionally related events that can influence the overall status of devices when they are triggered by these devices. Each event within an overall status group can be assigned an overall status that the device will adopt when the corresponding event condition occurs.

    You will find more detailed information on this function in the section Administration - Events Overall status groups (Page 200)

- Monitoring events
  - Event list

    The events list is used to monitor events. It shows the current statuses of the events enabled in SINEMA Server.

    Which events are displayed also depends on the views assigned to the currently entered user. This means that events of interest are only monitored in conjunction with the configured views.

    For events that are assigned to overall status groups, their event status is important. The event status indicates whether the event has an influence on the overall status of devices.

    By connecting the event list with a topology, specific devices for which events of the event list were triggered can be displayed in a graphic network representation.

    For more detailed information the events list, refer to the section
    Event list (Page 128)
  - Device details > Events

    An additional option for obtaining a device-specific overview of the status of the configured events is to use the display of the device details.

    You will find more detailed information on this function in the section Device details (Page 104)

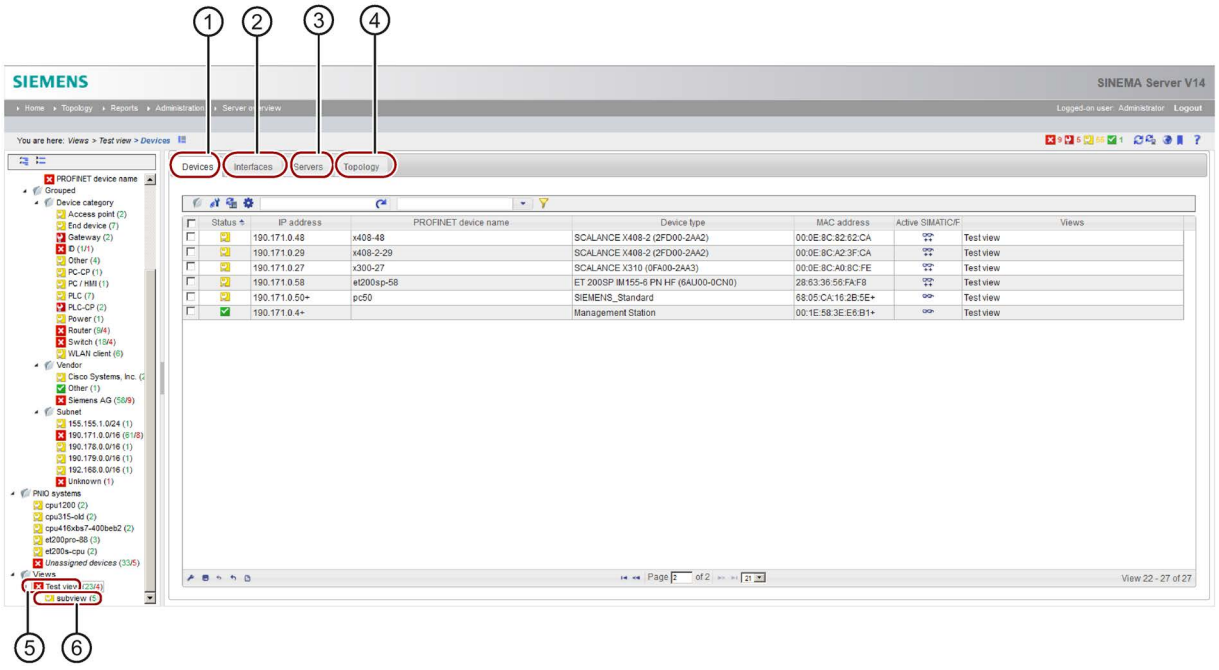
3.5 Setting up and using views

3.5.1 Setting up views

Views - purpose and use

Dividing up a large hierarchy of the network topology into small groups made up of several devices and SINEMA Server instances simplifies the management or monitoring of the devices and SINEMA Servers and their connections.

By assigning the views in the user management to individual users that do not have the right "View all devices and servers", the number of devices that can be monitored can be restricted for the specific user.



① View-specific device list
② View-specific interface list
③ View-specific list of SINEMA Server instances
④ View-specific topology
⑤ Basic views
⑥ Sub views

Aims

From the total monitored network, you set up separate monitoring groups with the following properties and options:

- Basic views

  Basic views provide a specific view of a section of the total monitoring.
- Sub views:

  When necessary, sub views provide further specific sections of the network.
- View-specific topology

  When necessary, set up a view-specific topology view.
- View-specific display in the events list (refer also to the section Event list (Page 128))

Requirements

To be able to set up views, the following requirements must be met:

- If you want to create a view-specific topology, a reference topology must exist.
- To include SINEMA Server instances in a view-specific topology, these must be created in the "Server overview" tab.
- User right: "Operative monitoring settings".

Creating a new view

Depending on the initial situation, two variants need to be distinguished:

Creating a basic view

1. Select the "Views" node.
2. With the right mouse button select the "Create new view" menu command; this opens the View editor.
3. Configure the new view in the Views editor by assigning the required devices and SINEMA Server instances to the view in the "Devices" and "Servers" tabs.

   SINEMA Server instances are only shown in the "Servers" tab if they have been created in the server overview. For more detailed information on the server overview, refer to the section Server overview (Page 239).
4. If in addition a view-specific topology display should be generated, enable the "Display topology" check box.
5. If necessary, configure the topology, see section Creating a view-specific topology (Page 65).

Creating a sub view

1. Select an existing view node.
2. With the right mouse button select the "Create new view" function; this opens the View editor.
3. Configure the new view in the View editor.
4. If in addition a view-specific topology display should be generated, enable the "Display topology" check box.
5. If necessary, configure the topology, see section Creating a view-specific topology (Page 65).

NOTICE
Deleting views When you delete a view, the view itself, all the sub views it contains and all assignments to users or event reactions are deleted.

Positioning views later

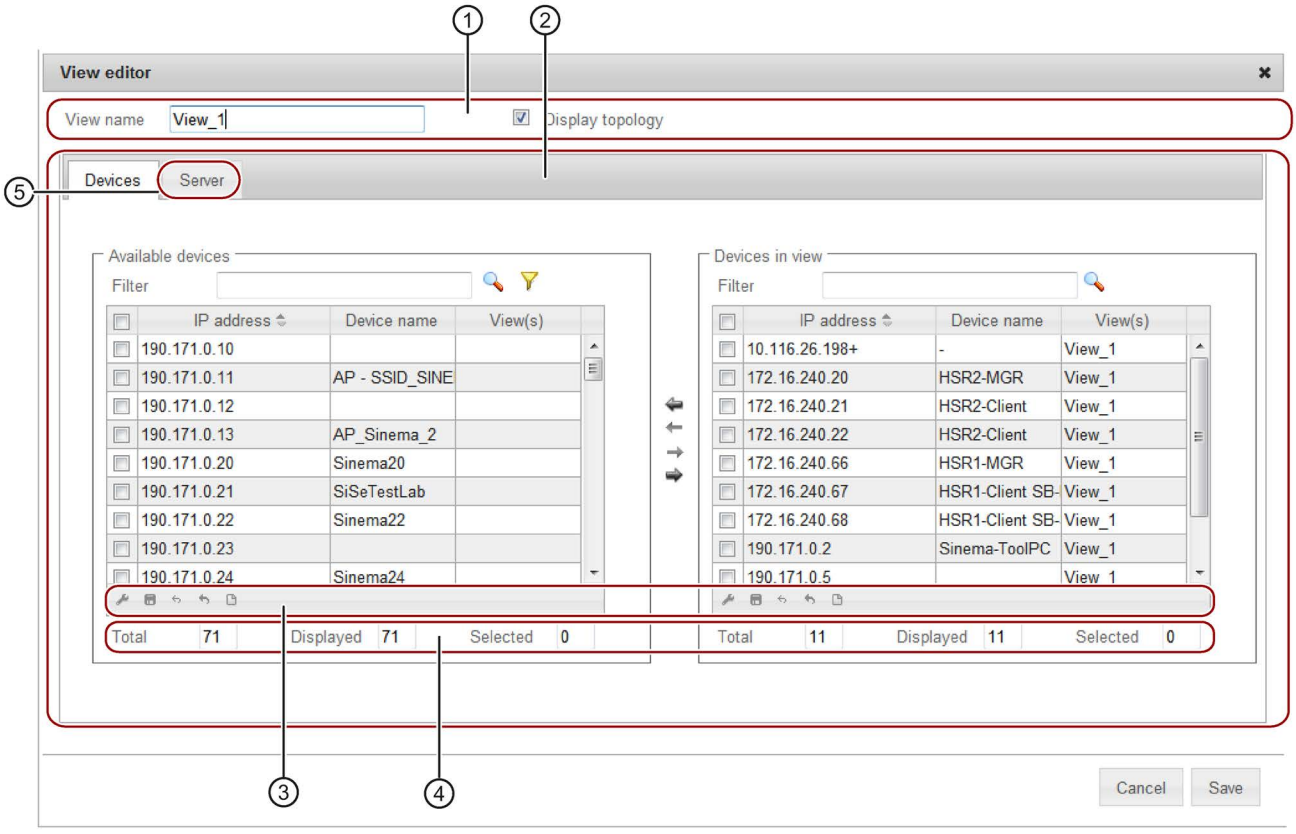
To move a view or a sub view to a different hierarchical position after they have been created, follow the steps below:

1. Select the "Views" node.
2. Right-click and select "Change view hierarchy" in the shortcut menu.
3. In the "Change view hierarchy" dialog, drag the views to the required position.

Using the arrow icon in the upper part of the dialog you can restore the last stored status.

3.5.2 The View editor

You open the View editor in the with the function for creating or editing a view. The way in which the Views editor works is the same for devices and SINEMA Servers instances.



① Header
② Assignment area
③ Settings area
④ Statistics
⑤ Views editor for SINEMA Server instances

How it works

In the "Devices" tab, take the devices to be included in the view from the list of "Available devices" and add them to the "Devices in view" list. Follow the same procedure in the "Servers" tab for SINEMA Server instances that were created in the server overview.

View filter for devices and SINEMA Server instances

The view filter allows you to preselect devices and SINEMA Server instances that have not yet been assigned to the current view.

The view filter provides the same filter options for devices and SINEMA Server instances. For this reason, the term "object" is used for both components in the following list:

- Show all objects (regardless of view).
- Display objects that are not part of a view (except for this view).

  The node with the user-specific views is also displayed and can be selected.

  Select the views whose objects should **not** be included in the "Available devices" or "Available servers" list box.
- Select views whose objects will be displayed.

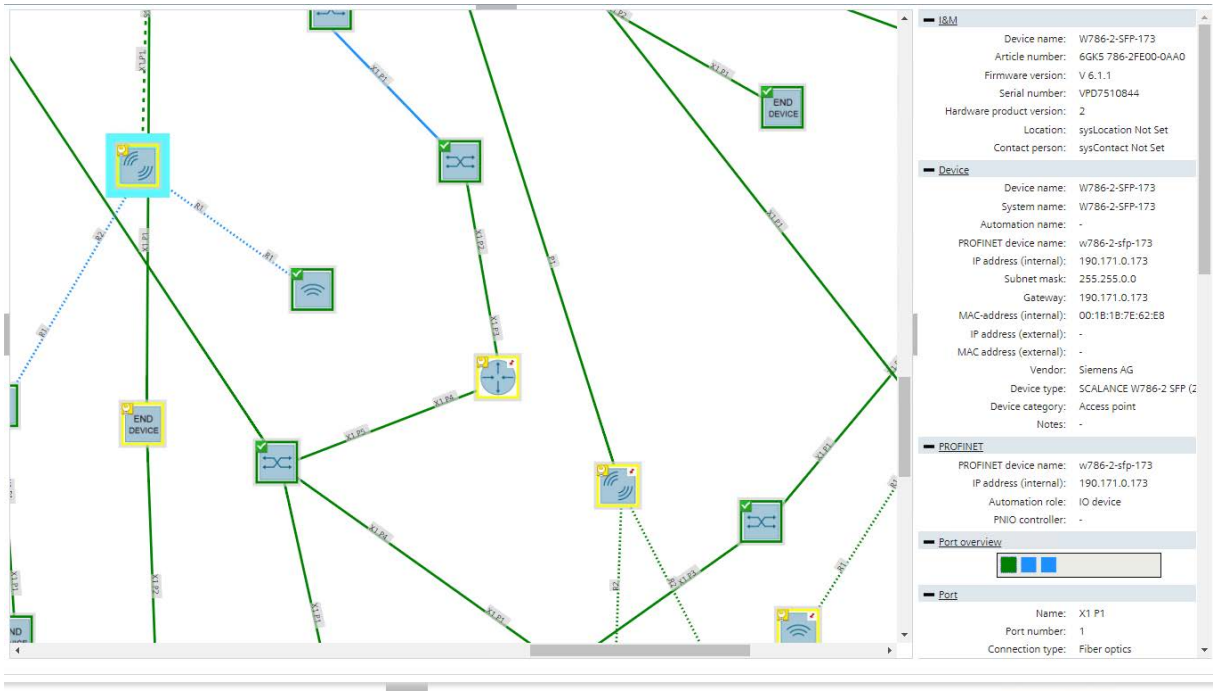
  The node with the user-specific views is also displayed and can be selected.

  Select the views whose objects should be included **exclusively** in the "Available devices" or "Available servers" list box.

3.5.3 Creating a view-specific topology

Overview

The topology of a view shows a section of the network, in which devices, SINEMA Server instances and sub views of this view are diplayed. Before view-specific topologies can be displayed, a reference topology must exist. Devices must be part of the reference topology to be able to be inserted in view-specific topologies. For the connections between inserted devices, SINEMA Server uses the configured reference connections. From the reference connections, user-defined connections can be created that are displayed when monitoring the view-specific topology.



Creating a view-specific topology

1. Select the created view in the device tree and select the "Topology" tab. This tab is available if you have enabled the "Display topology" check box in the View editor.
   The view-specific topology is displayed in the Editing mode. This is made clear by the icon.
2. In the "User-defined view" area the reference devices, sub views, SINEMA Server instances contained in the view and the unmanaged devices existing in the reference topology are displayed. Drag the required elements to the topology display. Between devices and unmanaged devices, the configured reference connections are shown.
3. Activate the selection tool and move the elements to the required positions. Using the icon, you can insert a background graphic to make the display clearer.
4. With the drawing tool , you can draw in user-defined connections manually between the inserted elements. SINEMA Server instances can only have manually drawn, user-defined connections to other SINEMA Server instances. As an alternative you can adopt the reference connections as user-defined connections with the icon. For individual connections, this is possible using the shortcut menu of reference connections.
5. With the selection tool using the shortcut menu of user-defined connections you can generate bending points and move them by dragging them. This allows the course of user-defined connections can be adapted.
6. Click the "Save" button and change to the Online mode using the icon .

In Online mode the elements inserted in Editing mode with their monitoring statuses for devices and ports and the user-defined connections drawn between them are displayed. Reference connections are not displayed in Online mode. Deviations between user-defined connections and discovered connections are not indicated in view-specific topologies.

3.6 Users and user groups

3.6.1 SINEMA Server users and roles concept

Overview

SINEMA Server has an extensive system of access rights. This system allows the administrator to grant or deny access to certain program objects individually and according to need. During configuration, you should take into account the following criteria in the role:

- Network security
- IT experience of the users
- The necessity for certain functions
- User friendliness

Note

Managing user rights is one of the main tasks of an administrator.

This should therefore be planned and configured to meet the specific requirements while taking into account security-relevant aspects. We strongly advise you to familiarize yourself with the user and roles concept of SINEMA Server. New or modified settings should always be checked in terms of their intended effect.

Basics

The access rights in SINEMA Server are specified using the following objects:

- User
- User groups
- Views

In principle, the following applies: Each user belongs to a user group. Each user group has certain rights that are transferred automatically to all its members (users). In addition, every user can be assigned so-called views via which the user is also granted certain rights.

Standard users and groups

In SINEMA Server, there are three predefined user groups with corresponding access rights. The control elements and options for the corresponding users differ in each user group. The following table shows the predefined name of the user group as well as information on the access rights:

Name of the user group	Access rights
Administrator	The administrator has all access rights available in SINEMA Server.
Power user	A power user has all the access rights of an administrator except for the user management rights.
Standard user	The standard user has the general access rights of an operator.

As default, the predefined user "Administrator" is available in SINEMA Server that is assigned to the user group of the same name.

The range of access rights when working with SINEMA Server depends on the user group to which the user belongs. The default assignment of rights to user groups is explained below:

Access right	Description	Administrator	Power user	Standard user
Server access via URL	Access right for the function call via URL As default, this right is disabled for all user groups. For security reasons, it should only be enabled for user groups with restricted access rights.	No	No	No
View reports	Access to the display of reports	Yes	Yes	Yes
Operative monitoring settings	Access right for monitoring and managing all devices, views and SINEMA Server instances and for using the topology (Editing and Online mode)	Yes	Yes	No
User settings	Access right allowing administration of users and user groups	Yes	No	No
Basic settings for discovery and monitoring	Access right for the basic discovery and monitoring settings	Yes	Yes	No
View user-specific topology	View devices and SINEMA Server instances of the views assigned to the user also in topology (only Online mode). Connections between devices that are not assigned are not displayed.	Yes	Yes	Yes
View all devices and servers	View all devices, SINEMA Server instances and validation reports, regardless of assignment of views, use topology (online mode only)	Yes	Yes	No
View server overview	Access right for the server overview	Yes	Yes	Yes
System settings	Access right for settings under "Administration > System"	Yes	Yes	No
All jobs and basic job settings	Create, edit, delete and execute all job types and make all basic job settings	Yes	Yes	No
Firmware download and activation	Create, edit, delete and execute jobs of the job type “Firmware download” and make basic job settings for this job type	Yes	Yes	No
CLI	Create, edit, delete and execute jobs of the job type “CLI” and make basic job settings for this job type	Yes	Yes	No
System backup	Edit and execute a job of the job type “System backup”	Yes	Yes	No
Database cleanup	Create, edit, delete and execute jobs of the job type “Database cleanup” and make basic job settings for this job type	Yes	Yes	No
View validation reports	View existing validation reports and validation report configurations	Yes	Yes	Yes

Access right	Description	Administrator	Power user	Standard user
Start and delete validation reports	• Start and delete validation reports • Copy validation report configurations and create them based on validation report templates • Edit basic settings of validation report configurations	Yes	Yes	Yes
Create and configure validation reports	Create, configure, and delete validation report configurations and templates	Yes	No	No
Comments and events	• Add or delete comments on devices and events • Resolve events manually	Yes	Yes	Yes

How it works

Whenever a user wants to execute a command, SINEMA Server checks whether or not the user has the right to do this. The following individual points are checked:

- Which user group does the user belong to?
- Does the group have the required right?

1. When necessary, create new user groups, see section Administration - Users user groups (Page 210)
2. Create new users and assign these to the required user groups, see also section Administration - User User (Page 208)

   When necessary, assign views to the users. As a result, the response of the Web user interface of SINEMA Server terms of the devices and SINEMA Server instances that can be monitored depends on the specific view.

Using SINEMA Server - reference section

4

4.1 Program user interface in detail - overview of the menus

4.1.1 User interface

This section provides you with an overview of the following:

- Menu commands with a brief explanation and references to other sections
- General functions for setting the page layout and for navigation within a Web page

Menu commands

The navigation bar has the following menu commands that are explained below

Start menu command	Meaning	See section
No other sub entries	The start window of SINEMA Server provides a quick overview of the status of the network.	Start window (Page 91)

Menu command Topology >...	Meaning	See section
...Topology	Visualization of the devices and network connections in a topology display. In the Editing mode you can configure a reference topology that can be used as the expected status of the network. In Online mode you can monitor the network taking into account the configured reference topology. If the topology has already been saved in the Editing mode, the topology display is opened in the Online mode after selecting the "Topology" menu command.	Topology (Page 134)
...Unmanaged devices	You can manage devices that cannot be monitored by SINEMA Server and that can be inserted In Editing mode to complete the topology display. These devices are then also displayed in Online mode.	Unmanaged devices (Page 149)

Menu command Reports >...	Tab	Meaning	See section
...Availability >	Devices	Display of all devices with information relating to their availability; in other words, how long they were reachable during the monitoring period.	Reports - Availability (Page 151)
	Interfaces	All the interfaces of the devices are displayed individually.	
...Performance >	LAN - Interface utilization	For all LAN interfaces, not only the possible speed but also their total load when sending and receiving is displayed.	Reports - Performance (Page 154)
	LAN - Interface error rate	The error quota when sending and receiving is displayed for all LAN interfaces.	
	WLAN - Interface error rate	The error quota when sending and receiving is displayed for all WLAN interfaces.	
	WLAN - Interface data rate	The transmission speed when sending and receiving is displayed for all WLAN interfaces.	
	WLAN - Signal strength	For all WLAN interfaces, the average signal strength is displayed.	
	WLAN - Number of clients	For all access points, the number of WLAN clients to which they were connected on average is displayed.	
	Discarded packets	The number of discarded incoming packets and the number of discarded outgoing packets is displayed for all LAN and WLAN interfaces.	
	POF power margin:	For all LAN interfaces of the type "Plastic Optical Fiber (POF)", information about the power margin is displayed.	
...Inventory >	Vendor	Overview of the devices according to the manufacturer identifier.	Reports - Inventory (Page 156)
	IP address range	Overview of the devices according to IP address ranges.	

Menu command Reports >...	Tab	Meaning	See section
	Device category	Overview of the devices according to device types (switch etc.)	
	PROFINET	Overview of the devices that have a PROFINET name.	
...Events >	Network events	Display of all the events that have occurred with information relating to the status, event type and the time the event occurred.	Reports - Events (Page 157)
	System events		
...Validation reports >	Validation report configurations	Management of validation report configurations and generation of the corresponding validation reports	Reports - validation reports (Page 159)
	Validation report templates	Management of templates for validation report configurations	

Menu command Administration >...	Tab	Meaning	See section
...Discovery >	Scan	Here, you set the parameters for the network scan and start the scan.	Administration - Discovery / Scan (Page 174)
	Profiles	You can edit displayed profiles or add new profiles.	Administration - Discovery / Profiles (Page 177)
...Monitoring >	General	Here you set the time parameters for network monitoring and globally enable the monitoring modes for devices with SIMATIC and PROFINET capability and configure display texts for PROFINET diagnostics.	Administration - Monitoring General (Page 186)
	SNMP settings	Basic settings for discovery using the SNMP protocol.	Administration - Monitoring SNMP settings (Page 191)
	Polling groups > Fast / Medium / Slow	Depending on the requirements, assign the devices to the 3 possible polling groups.	Administration - Monitoring Polling groups (Page 193)
	OPC	Select devices whose data will be sent to an OPC server.	Administration - Monitoring OPC (Page 196)
...Events	Event types	Make the settings for the display and representation of the network and system events.	Administration - Events (Page 198)
	Overall status groups	View / configure groups of functionally related events that influence the overall status of devices.	Administration - Events Overall status groups (Page 200)

Menu command Administration >...	Tab	Meaning	See section
	Event reactions	Define view-specific, system- and device-specific reactions to events.	Administration - Events > Event reactions (Page 205)
	Syslog server	Configure Syslog servers to which SINEMA Server forwards triggered events.	Administration - Events Syslog Server (Page 207)
...User	User	Assign users to groups and views.	Administration - User User (Page 208)
	User groups	Create user groups with rights.	Administration - Users user groups (Page 210)
	Logon locks	Cancel logon locks for users and IP addresses	Administration - User Logon locks (Page 212)
...System	System information	Display information about the management station	Administration - System System information (Page 212)
	Configuration	Functions for saving, importing or resetting the configuration data of SINEMA Server and for specifying the shared secret.	Administration - System configuration (Page 212)
	E-mail settings	Specify e-mail settings required for event reactions.	Administration - System / E-mail settings (Page 214)
...My settings	Password	Changing your password	Administration - My settings Password (Page 219)
	User interface	Here, you specify the update interval for all user interface components relevant for monitoring.	Administration - My settings User interface (Page 219)
...Jobs	No other sub entries	Management and control of jobs for management tasks	Administration - Jobs (Page 220)

Server overview menu command	Meaning	See section
No other sub entries	Display of the overall statuses of devices monitored by other SINEMA Server instances in the network. These SINEMA Server instances can be called directly from the server overview.	Server overview (Page 239)

General functions for the page layout

All tables have a footer with which you can specify the page layout. Other functions are used for navigation within the particular Web page.

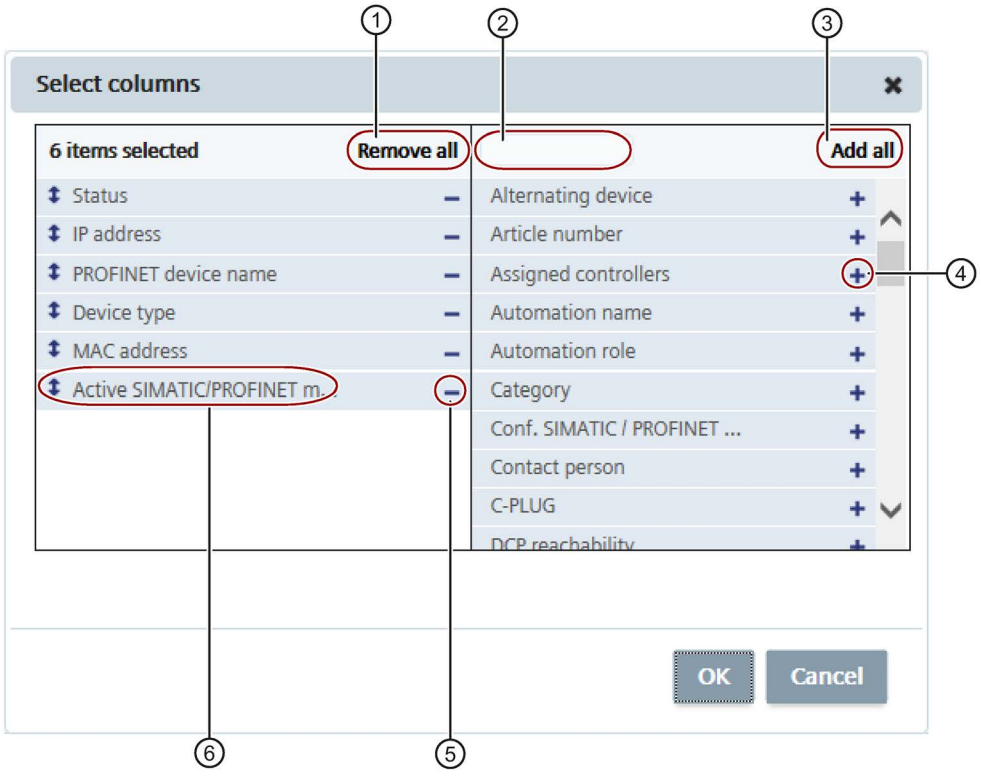
Depending on the particular Web page, you have a selection of the following functions:

Icon	Display / function	Icon	Display / function
	Select and position columns for display.		User-specific saving of the following user interface parameters: • Column selection • Column order • Column width • Column sorting • Number of entries per page • Filter setting using a selection list
	Select saved column layout.		Use default column layout
	Export table in CSV format		Go to first page.
	Go back one page.		Display the current page and option to scroll directly to specific page.
	Go forward one page.		Go to last page.
	Specify how many rows to display per page.		

General functions for the table layout

In a series of Web pages, information is shown in the form of a table. SINEMA Server provides functions for individual structuring of the table display.

You can see the possible settings for the display in the tables of the following graphic:



① Selection option - remove all columns from the table. At least 1 column must be selected again.

② Input option for character strings - only the elements that contain the specified character string are displayed

③ Selection option - add all columns to the table.

④ Select "+" to add an individual entry as a column in the table

⑤ Select "-" to remove an individual column from the table.

⑥ Move entries up or down using the mouse cursor to change the order of the columns and table.

Selecting entries in tables

The first column of every table contains a check box. This check box is available in the header as well as in every row of the table.

Follow the steps outlined below to select table entries.

- Select single entry

  Click the check box in the table row. You can use this to select an individual entry and deselect other selected entries.

- Select multiple entries (range)

  Holding down the shift key, click the check box of the first and last entry in the contiguous table range.

- Select separate multiple entries

  Holding down the Ctrl key, click the check box of the required entry.

- Select all entries of the same page

  Click the check box in the header.

- Deselect single entries

  Holding down the Ctrl key, click the check box of the selected entry.

4.1.1.1 Filtering data with filter templates

Function of filter templates

Data displayed in SINEMA Server can be filtered according to various criteria. To avoid needing to configure the selected filter criteria again before every filtering action, you can store these in a filter template and reuse the filter template. Cross-user filter templates can be reused by all users of the SINEMA Server instance.

Settings of filter templates

The settings that can be made in a filter template can be divided into three categories. The criteria of these categories are applied to the data to be displayed in the order shown below.

1. Prefilters

   The prefilter contains basic filter criteria to be used at the server end on data to be displayed. Data that passes the prefilter is forwarded to the clients.

2. Complex filter

   The data received by the clients is filtered in the second step using a complex query if this exists. With a complex query, filter rules can be created for individually selectable columns. These rules can be logically linked using logical operators and nested in one another by using the rule levels.

3. Simple filter

   The data that has passed the complex filter is filtered in the third step by a free text entry. In contrast to the complex filter, as default the simple filter includes all columns of the relevant data category.

Use of filter templates

Filter templates can be used to filter the following lists:

- Event list
- Device list
- Interface list
- Reports

In the course of the relevant section, the prefilter settings will be described in greater detail. The control elements of the editor for filter templates and for complex filters are described below. These are identical for all lists to be filtered.

Control elements of the filter template editor

The following table explains the functions of the control elements of a filter template.

Control element / tab name	Function
Simple filter	Filter data using a free text entry. All columns of the relevant data category are included.
Complex filter	The dialog for creating a complex filter query opens; refer to the section "Control elements of the editor for complex filters".
Prefilters	Prefilter settings for filtering the data to be displayed at the server end. The prefilter settings are described in greater detail in the relevant sections on the event list, device list, interface list and reports.
Delete	Deletes the open filter template
Save	Saves the configured filter settings for the open filter template. System-defined filter templates can only be changed by users with the right "System settings".
Save as	Opens a dialog for entering a name for the filter template under which the configured filter settings will be saved. The name must be unique in the SINEMA Server instance and can contain a maximum of 25 characters. If you enable the "Cross-user filter template" check box in this dialog, the filter template can be used by every user who has the "System settings" right. Per list type a maximum of 10 user-specific and 10 cross-user filter templates can be created.
Cancel	Discards changes to the open filter template and closes the filter template and template editor.
Reset filter	Discards changes to the open filter template and closes the filter template.
Use filter	Applies the configured filter settings to the list to be filtered.

Control elements of the editor for complex filters

The editor for creating a query for the complex filter is opened with the  icon. In the open filter editor, complex filters can be created with the following control elements. Created filters are displayed in the "Complex filter" area of the filter template textually.

Operator control element	Function
Complex filter	Textual representation of the created filter. The textual representation is updated when using the control elements of the editor.
	As an alternative to using the buttons and drop-down lists of this editor, the filter text can also be edited manually. Using the arrow icon, the modified filter text is validated and adopted for the control elements of the editor.
	Specifies whether the filter rules of the current rule level will be linked with the logical operator "AND" or "OR".
	Inserts a new rule level below the current rule level. Filter rules can be nested within each other using rule levels. Filter rules of the same rule level are shown in the query box in a common bracket.
	Inserts a new filter rule at the current rule level. Every filter rule contains a selectable column name, a selectable operator and an input box in which the value of the selected column to be checked with the operator can be entered.
	Deletes the rule level or the filter rule.
Cancel	Discards changes to the open complex filter and closes the filter editor.

Operator control element	Function
Reset	Discards changes to the open complex filter.
Apply	Saves the settings for the complex filter and closes the filter editor. The created complex filter is now displayed in the "Complex filter" box of the filter template editor.

4.1.2 Online help

Opening help pages

You have the following options:

- Opening a context-dependent page

  On every Web page in SINEMA Server, you can display a page of the online help describing the current context by clicking the question mark icon in the status bar. In addition to this, in the "Device details" window, the shortcut menu command "Open help" is available to open the help page for the device details.

- Opening any help page - navigating in the online help

  After you have opened a context-dependent help page, you can navigate to any help pages of SINEMA Server with the navigation panel on the left hand side.

- Opening a topic-related help page (only with Internet Explorer)

  In most help pages, you can open other help pages relating to the current topic with the "Basics" menu command.

Note

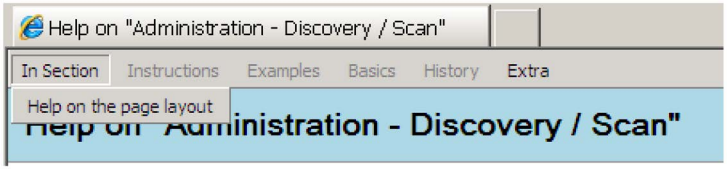
Opening using the question mark icon - new window in the Web browser

Every help page you open using the question mark icon opens in a new window of your Web browser.

This does not apply to help pages you open using the menu commands in the open online help described below.

Menu commands

The open online help has further menu commands in the header for navigation.



Menu command	Meaning
In Section > ...	Option for selecting sections in the open help page
Instructions	- not used -
Examples	- not used -
Basics	Option for opening help pages whose content is related to the topic of the selected help page.
History > ...	Option for selecting previously opened help pages.
Extra	Opens the navigation page of the online help. From the navigation page, you can open all the help pages of the online help of SINEMA Server.
Extra > Back	Opens the previously opened help page.
Extra > Next	Opens the next help page in the history of previously opened help pages following the currently open help page. If the currently displayed help page is the last page in the history, the menu command has no effect.

Note

Opening help pages using "History" or "Extra"

The history only includes help pages that have already been opened in the currently open Web browser window and only these can be selected.

4.1.3 Quick links

Meaning

With the "Quick links" function element , you can manage and use fast access to SINEMA Server Web pages you require often.

You can assign quick links for all standard Web pages and for view-specific Web pages.

Setting up a quick link

To assign quick links for Web pages and to specify a start page for SINEMA Server, follow the steps below:

1. Select the Web page you want to open using a quick link.
2. Select the "Quick links" function element

   You open the list of available quick links.
3. Click the "New" button.

   This opens the "Quick links" dialog and the menu command of the currently displayed Web page is shown.

4. Assign a name for the Web page that you would like entered in the list of quick links.
5. As an option, you can define one of the created direct references as the start page with the "Start page" button.

Using a quick link

To call up a Web page of SINEMA Server directly, follow the steps below:

1. Select the "Quick links" function element

   You open the list of available quick links.
2. Double-click on the required quick link.

   You open the Web page.

4.1.4 Calling functions with a URL

Overview

You can call up certain functions of SINEMA Server in the Web browser by specifying the URL directly and adding the login data. In this case, you do not need to log in with SINEMA Server first. The login is made in conjunction with the call for the relevant Web page.

The following actions are possible:

- Call for a specific Web page
- CSV/JSON download of the content of a Web page

Per management station URL function calls from a maximum of 50 users simultaneously are supported.

Authentication - logging in with SINEMA Server

Requirement for access

- SINEMA Server must be running on the management station that is addressed using the URL.
- To have direct access to SINEMA Server using the URL, you need to be a member of a user group with the "Server access via URL" access right.

In the URL, enter the user name and the user-specific password. This entry is case sensitive.

You have the following options for logging in:

- You first send a separate call for the login. SINEMA Server then opens a session with the logged in user. After this, you can enter other URLs without needing to enter the login data again.

  Example:

  – "https://150.25.10.145:443?username=johndoe&password=hello123"

    with the following significance:

    IP address = 150.25.10.145

    Default port = 443

    Login = username=johndoe&password=hello123

- You send the login data when you call a Web page.

NOTICE
Recommendation When entering the login data, we strongly advise you to use the HTTPS protocol for security reasons. The data is transferred encrypted and cannot be read by unauthorized third persons.

Basic parameters for calling Web pages

Below there is an example of a call for a specific Web page. The parameters used in this are explained in the following table.

Example: Display of the details of a device with the specified IP address

"https://sinemaserver:443?path=device_details&ip=192.168.110.34&username=john&password=blue&onlycontentarea=yes"

Table 4- 1 Basic parameters for the Web page call

Parameter	Meaning
path	Path of the SINEMA Server Web page to be displayed, see section below.
ip	IP address of a device. The IP address needs to be included in the URL in the following situations: • If the device details of a specific device should be included • If you want a specific device to be displayed after the topology display is opened.
username	Name of the user logging on
password	Password of the user logging on
onlycontentarea	Specifies whether or not only the SINEMA Server main window is displayed. YES: Only the main window is displayed.

Parameter "path"

Calling topology-relevant Web pages is supported by the following software versions:

- WinCC RT 7.4 and higher
- WinCC RT V13 SP1 and higher (only Webkit mode)

Path	Called Web page
path=main_logout	The user that calls the function is logged out of the SINEMA Server instance. The function call applies only for the session in which it occurs. Other sessions remain unaffected by the function call.
path=main_kill_session&username=Administrator&password=SinemaA	End all sessions of a user. Note: The parameters for user name and password must be specified with this function call. In the example shown, the user name is "Administrator" and the password "SinemaA".
path=mnu_admin_event&tabname=admin_condition_grp	Administration > Overall status groups
path=mnu_new_topology	Topology > Topology (Online mode)
path=mnu_reports_availability	Reports > Availability > Devices
path=mnu_reports_performance	Reports > Performance > LAN - Interface utilization
path=mnu_reports_inventory	Reports > Inventory > Vendor
path=mnu_reports_events	Reports > Events > Network events
path=mnu_Server_overview	Server overview
path=views_tabs&params=views_{view name}	Shows the named user-specific view. The device list is displayed.
path=views_tabs&params=views_{view name}&tabname=views_topology	Shows the named user-specific view. The view-specific topology is displayed in the Online mode.
path=device_list&params=alldevices_ipAddress	Device list with devices that have the specified IP address.
path=device_list&params=alldevices_profinet	Device list with devices that have the specified PROFINET device name.
path=device_list&params=devicetype_{device type}	Device list with devices of the named device type
path=device_list&params=local_Not Connected	Device list with devices with the "Not connected" status
path=device_list&params=local_Ok	Device list with devices with the "OK" status
path=device_list&params=local_Fault	Device list with devices with the "Fault" status
path=device_list&params=local_Maintenance demanded	Device list with devices with the "Maintenance demanded" status
path=device_list&Params=local_Maintenance required	Device list with devices with the "Maintenance required" status
path=device_list&Params=local_Not reachable	Device list with devices with the "Not Reachable" status

Path	Called Web page
path=device_list&Params=local_Not Monitored	Device list with devices with the "Unmonitored" status
path=device_list&params=pniosystems_{name of PNIO system}_{ip address as shown in tooltip}	Device list with devices of the named PNIO system
path=device_list&params=vendor_Siemens AG	Device list with devices of the "Manufacturer / Siemens AG" category
path=device_list&params=vendor_Microsoft	Device list with devices of the "Manufacturer / Microsoft" category
path=device_list&params=vendor_ciscoSystems	Device list with devices of the "Manufacturer / Cisco systems" category
path=device_list&params=vendor_others	Device list with devices of the "Manufacturer / Unknown" category
path=device_list&params=Subnet_{network address and subnet mask in CIDR notation, e.g. 192.168.100.0/24}	Device list with devices of the subnet 192.168.100.0/24
{call up a device list}&tabname=interfaces	Opening the interface list from one of the device lists mentioned above
path=device_details&ip={ip address}	Details of the device with the specifies IP address
path=device_details&ip={ip address}&tabname=summary	Device details in the "Overview" tab
path=device_details&ip={ip address}&tabname=status	Device details in the "Status" tab
path=device_details&ip={ip address}&tabname=desc	Device details in the "Description" tab
path=device_details&ip={ip address}&tabname=simatic	Device details in the "SIMATIC" tab
path=device_details&ip={ip address}&tabname=profinet	Device details in the "PROFINET" tab
path=device_details&ip={ip address}&tabname=settings	Device details in the "Config." tab
path=device_details&ip={ip address}&tabname=lan	Device details in the "LAN port" tab
path=device_details&ip={ip address}&tabname=wlan	Device details in the "WLAN" tab
path=device_details&ip={ip address}&tabname=events	Device details in the "Events" tab
path=device_details&ip={ip address}&tabname=vlan	Device details in the "VLAN" tab
path=device_details&ip={ip address}&tabname=redundancy	Device details in the "Redundancy" tab
path=device_details&ip={ip address}&tabname=interfaces	Device details in the "Interfaces" tab
path=device_details&ip={ip address}&tabname=expert	Device details in the "Exert" tab
path=events	Event list

Parameter for calling up trend diagrams of SINEMA Server instances of the server overview

Using function calls, the trend diagrams of SINEMA Server instances that exist in the server overview can be displayed. The trend diagrams show the numbers of overall statuses of devices that are monitored by the specified SINEMA Server instance. The representation in the trend diagrams is optimized for display in Web browsers on SIMATIC HMI devices. The representation therefore only takes the last 24 hours into account and the statuses "Maintenance required", "Maintenance demanded" and "Unreachable".

Below there is an example of the call for a trend diagram of a SINEMA Server instance from the server overview. The parameters associated with this are explained in the following table.

Example: Call for the trend diagram of the SINEMA Server instance "SINEMAServerLab" with a width of 400 pixels and a height of 300 pixels.

"https://localhost:443?username=johndoe&password=SINEMA&path=mnu_Server_overview&TrendChartForServerName=SINEMAServerLab&width=400&height=300"

TrendChartForServerName={name of the server}	Selection of the SINEMA Server instance via its name in the Server overview
TrendChartForIp_host={IP address or computer name of the server}	Selection of the SINEMA Server instance via its IP address/ computer name
width	Optional specification of the width of the window for the trend diagram Minimum value: 250 (default value) Maximum value: 1980
height	Optional specification of the height of the window for the trend diagram Minimum value: 200 (default value) Maximum value: 1080

Basic parameters for the CSV/JSON download of the content of a Web page

Below there is an example of the download of a specific Web page. The parameters used in this are explained in the following table.

Example: CSV download of the content of the Web page "Reports > Availability > Devices" in English specifying the start and end date to be taken into account:

"https://localhost/exportTable?command=Sinema_GetReports&username=user&password=user123&report_type=4&report_startDate=2015-02-04 10:16:03&report_endDate=2015-02-05 10:16:03"

Table 4- 2 Basic parameters for the Web page download

Parameter	Meaning
exportTable?	Indicates that this is a download of Web page content.
command	Indicates which Web page type should be downloaded. The following are available: • Reports • Event list • Device list • Interface list The values of this parameter and the filter parameters are described in the tables below.
username	Name of the user logging in
password	User-specific password

Parameter	Meaning
language	Display language of the content to be downloaded. Possible values: • de • en • fr • zh Default setting if the parameter is not used: en
download	Format for the download. Possible values: • csv • json Default setting if the parameter is not used: csv

Parameters for downloading reports

Parameter	Meaning
command=Sinema_GetReports	Indicates the download of reports.
report_type	Indicates the report type to be downloaded. The values of the individual report types are: • Availability > Devices: 4 • Availability > Interfaces: 5 • Performance > LAN - Interface utilization: 6 • Performance > LAN - Interface error rate: 7 • Performance > WLAN - Interface error rate: 9 • Performance > WLAN - Interface data rate: 8 • Performance > WLAN - Signal strength: 10 • Performance > WLAN - Number of clients: 11 • Performance > Discarded packets: 33 • Performance > POF power budget: 39 • Inventory > Vendor: 1 • Inventory > IP address range: 2 • Inventory > Device category: 3 • Inventory > PROFINET: 38 • Events > Network events: 12 • Events > System events: 13 The possible filter parameters for event reports are described in the table below.
report_endDate	End date for the report data to be downloaded Format: yyyy-mm-dd hh:mm:ss

Parameter	Meaning
report_startDate	Start date for the report data to be downloaded Format: yyyy-mm-dd hh:mm:ss
period	Period for the data to be downloaded. Possible values: • 24 hours: 1 • 7 days: 2 • Unlimited: 3 Default setting if the parameter is not used: 1 For the download of event reports, parameter values 1 and 2 indicate the unit for the period to be filtered, see below.

The parameters for the start or end date and the period should not be specified at the same time.

Filter parameters for downloading events reports

Associated reports:

- Events > Network events (report_type: 12)
- Events > System events (report_type: 13)

Parameter	Meaning
eventNoted	Filter according to the status "Read": • Yes: 0 • No: 1 • All: 2 Default setting if the parameter is not used: 2
eventPendingStatus	Filter according to event statuses: • All: 0 • Not present: 1 • Resolved automatically: 3 • Resolved manually: 4 • Pending: 5 Default setting if the parameter is not used: 0
classFilter	Filter according to event classes: • Notification: Notification • Information: Info • Warning: Warning • Error: Error • All: All

Parameter	Meaning
protocolFilter	Filter according to protocols: • ICMP • DCP • ARP • SNMP • SNMP trap • Profinet • SIMATIC • SIMATIC Diag. Events • Multiple protocols: Computed • SIMATIC Alarms • All: All Default setting if the parameter is not used: All
period	Unit for the filter period: • Hours: 1 • Days: 2 • Unlimited: 3 Default setting if the parameter is not used: 1
periodValue	Filter period: • Possible range of values for hours: 1...24 • Possible value range for days: 1...7 If the value 0 is specified or the "periodValue" parameter is not used, the default value for the specified unit is used. • Default value for unit "Hours": 24 • Default value for unit "Days": 7

Multiple parameter values can be specified separated by commas.

Further filter parameters for downloading reports

Associated reports:

- Availability > Interfaces (report_type: 5)
- Performance > LAN - Interface utilization (report_type: 6)
- Performance > LAN - Interface error rate (report_type: 7)
- Performance > Discarded packets (report_type: 33)

Parameter	Meaning
fromIp	Filter according to "From IP address"
toIp	Filter according to "To IP address"
deviceName	Filter according to device names
deviceType	Filter according to device types

Parameter	Meaning
reportsCategory	Filter according to device categories: • End Device • Router • Switch • Gateway • Access Point • WLAN Client • PLC • PC/HMI • PC-CP • PLC-CP • Ident • Motion • Power • Others • All Default setting if the parameter is not used: All
statistics	Filter according to ports on which port statistics are activated or deactivated: • All: All • Port statistics enabled: Yes • Port statistics disabled: No Default setting if the parameter is not used: All
deviceFilter	Filter according to devices: • All devices: All • Existing devices: existing Default setting if the parameter is not used: All This filter parameter is available for all reports.

Multiple parameter values can be specified separated by commas.

Parameters for downloading event lists

Parameter	Meaning
command=Sinema_GetEvents	Indicates the download of event lists.
eventNoted	Filter according to the status "Read": • Yes: 0 • No: 1 • All: 2 Default setting if the parameter is not used: 2

Parameter	Meaning
eventPendingStatus	Filter according to event statuses: • All: 0 • Not present: 1 • Resolved automatically: 3 • Resolved manually: 4 • Pending: 5 Default setting if the parameter is not used: 0
period	Unit for the filter period: • Hours: 1 • Days: 2 • Unlimited: 3 Default setting if the parameter is not used: 1
periodValue	Filter period: • Possible range of values for hours: 1...24 • Possible value range for days: 1...7 If the value 0 is specified or the "periodValue" parameter is not used, the default value for the specified unit is used. • Default value for unit "Hours": 24 • Default value for unit "Days": 7
CategoryFilter	Filter according to event categories: • Network events: Network • System events: System • All: All Default setting if the parameter is not used: All
protocolFilter	Filter according to protocols: • ICMP • DCP • ARP • SNMP • SNMP trap • Profinet • SIMATIC • SIMATIC Diag. Events • Multiple protocols: Computed • SIMATIC Alarms • All: All Default setting if the parameter is not used: All
startDate	Start date for event list to be downloaded Format: yyyy-mm-dd hh:mm:ss
endDate	End date for event list to be downloaded Format: yyyy-mm-dd hh:mm:ss

The parameters for the start or end date and the period should not be specified at the same time.

Multiple parameter values can be specified separated by commas.

Parameters for downloading device lists

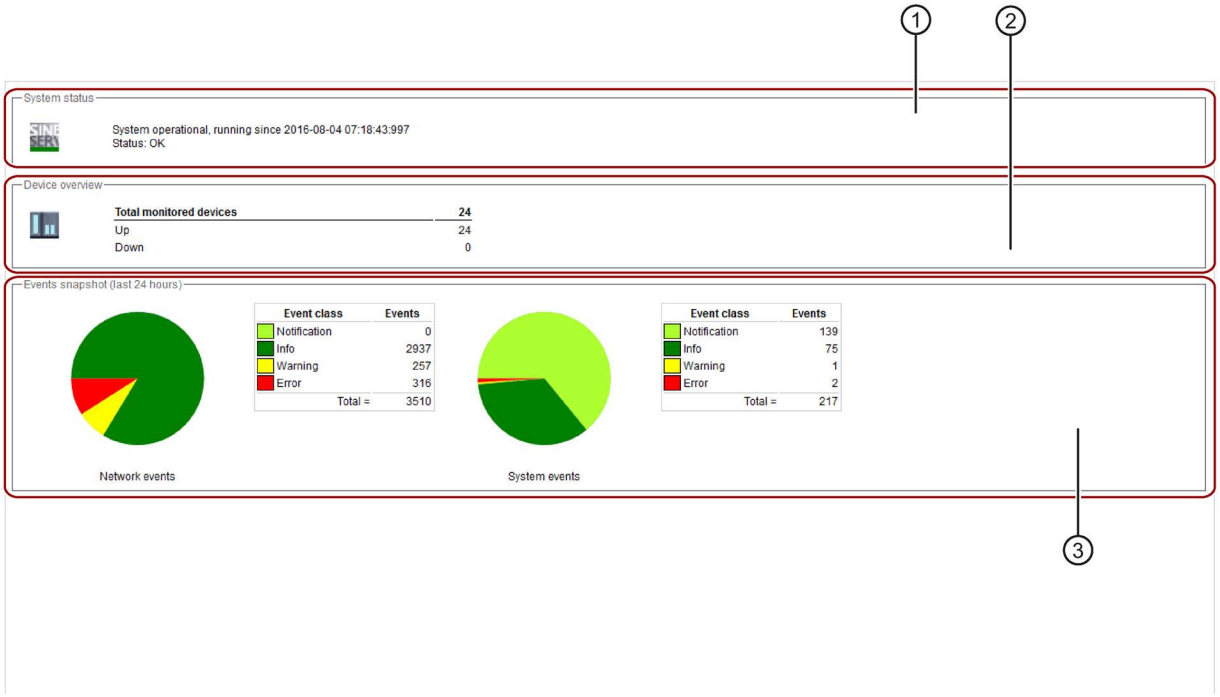
Parameter	Meaning
command=Sinema_GetDevices	Indicates the download of device lists.

Parameters for downloading interface lists

Parameter	Meaning
command=Sinema_GetInterfaces	Indicates the download of interface lists.

4.1.5 Start window

You open the Web page using the menu command: **"Begin"**



① System status
② Device overview
③ Event overview - grouped according to network events and system events

Layout

The start window of SINEMA Server provides a quick overview of the status of the network. Information on the availability of the devices and statistics of the last event are supplemented by general information about SINEMA Server.

Operation / content

The start window provides the following information and options:

- ① System status

  Information about how long (since which date and time) the SINEMA Server has been running.

  Current system status. Using the button of the SINEMA icon and its status text, information about the current system status can be displayed if problems occur.

  Note

  Critical system statuses

  The system statuses displayed when there is not enough work memory or hard disk space have the following meanings:

  - Server hardware: Work memory full, no more memory space available (caution): Work memory ≤ 200 MB
  - Server hardware: Hard disk full, no more memory space available (caution) / server hardware: No hard disk space available for archiving (caution): Hard disk space ≤ 300 MB

- ② Device overview

  Displays the number and status (active, inactive) of the monitored devices.

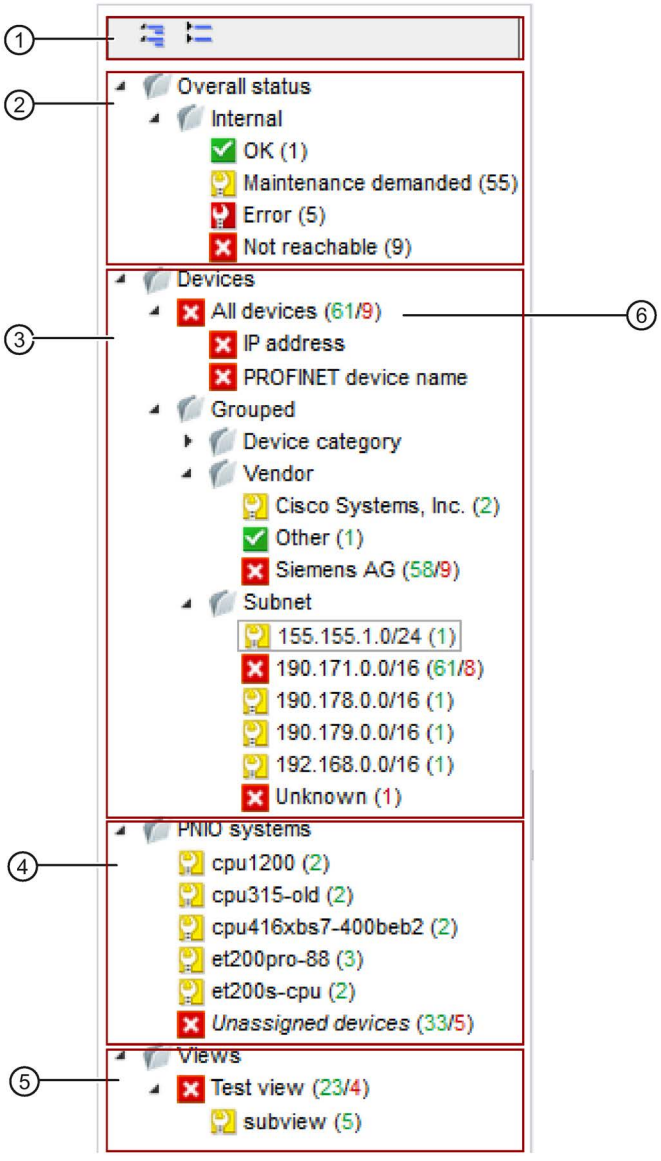
- ③ Events snapshot

  Overview of the number and type (error, warning, information, notification) of unread events, divided into network and system events.

4.1.6 Device tree

The device tree shows a navigation area for selecting device lists that are displayed after they are selected in the "Devices" tab of the device window. The "Interfaces" tab of the device window contains information about the LAN/WLAN attachments of the devices selected in the device tree.

The icons in the for the overall status in the device tree always show the worst current status of one of the device nodes in the branch.



① Button for expanding or collapsing the nodes

② Device nodes with filters for overall statuses of devices of this and other SINEMA Server instances

③ Device nodes for all devices and device nodes with filters for device categories, vendor, subnets and alternating devices

④ Device nodes for PROFINET IO systems

⑤ Node for user-specific views

⑥ Specifies the number of nodes contained in the particular device branch

Layout

- "Overall status" node:

  Below the "Overall status" node, the numbers of overall statuses of local devices as well as the devices monitored by other SINEMA Server instances are shown. Selecting an

overall status below the "Local" entry generates a filtered display of the device or interface window according to the overall status. Selecting an overall status below the "Server overview" entry generates a sorted display of server overview according to the overall status.

- "Devices" node:

  The entries below the "Devices" node provide the option of displaying all devices or only devices of a specific category, a specific vendor, a specific subnet or only alternating devices in the devices and interfaces window.
  For grouping according to subnets, the IPv4 addresses and subnet masks of the devices are used. External IP addresses configured for NAT routers are also included in the subnet grouping and after the subnet is selected they are displayed in the device list. For SCALANCE S devices this is only possible when the SINEMA Server has access via the external subnet. The subnet grouping with IPv6 addresses is not supported.
  The colors of the numbers in brackets indicate the reachability statuses of the devices.

- "PNIO systems" node:

  The entries below the "PNIO systems" node provide the option of displaying only the controller and the PROFINET IO devices of a certain PROFINET IO system.

  A CPU with SIMATIC capability that is configured as controller in multiple PROFINET IO systems is displayed in each of these PROFINET IO systems.
  The PROFINET interface modules of an HA PROFINET IO device that is integrated into multiple PNIO systems are displayed in each of these PNIO systems. SINEMA Server treats each PROFINET interface module of an HA PROFINET IO device as a separate device.

  Each PROFINET IO system is named after the PROFINET device name of the respective controller and indicates the overall statuses of associated PROFINET IO devices with the help of colored numbers in parentheses. The requirements for displaying a PNIO system are described in the section "Options for displaying PROFINET I/O systems".

  Using the shortcut menu command "Create PNIO view", you can create a view for the devices of a PNIO system. In the views editor that opens after selecting the shortcut menu command, the devices of the PNIO system are already assigned to the view. Passively monitored devices are excluded. Changes made to the PNIO system after creating the view have no effect on the view created for the PNIO system. Changes to a PNIO view have no effect on the PNIO system.

- "Views" node:

  For certain purposes, you can define user-specific views that include only some of the existing devices or only part of the overall network. You will find additional information on this topic in the section "Views (Page 125)".

Status information

In the device tree, you have an overview of the statuses of the devices monitored in the network. The icons in the device tree always show the worst current status of one of the device nodes in the particular branch.

Icon for the status	Description
	Device status: Not connected See section Alternating devices (Page 120)
	Device status: OK
	Device status: Maintenance required
	Device status: Maintenance demanded
	Device status: Error
	Device not reachable

Options for displaying PROFINET IO systems

Depending on which controller is used in a PROFINET IO system, this can be displayed in different ways:

- Devices with SIMATIC capability:

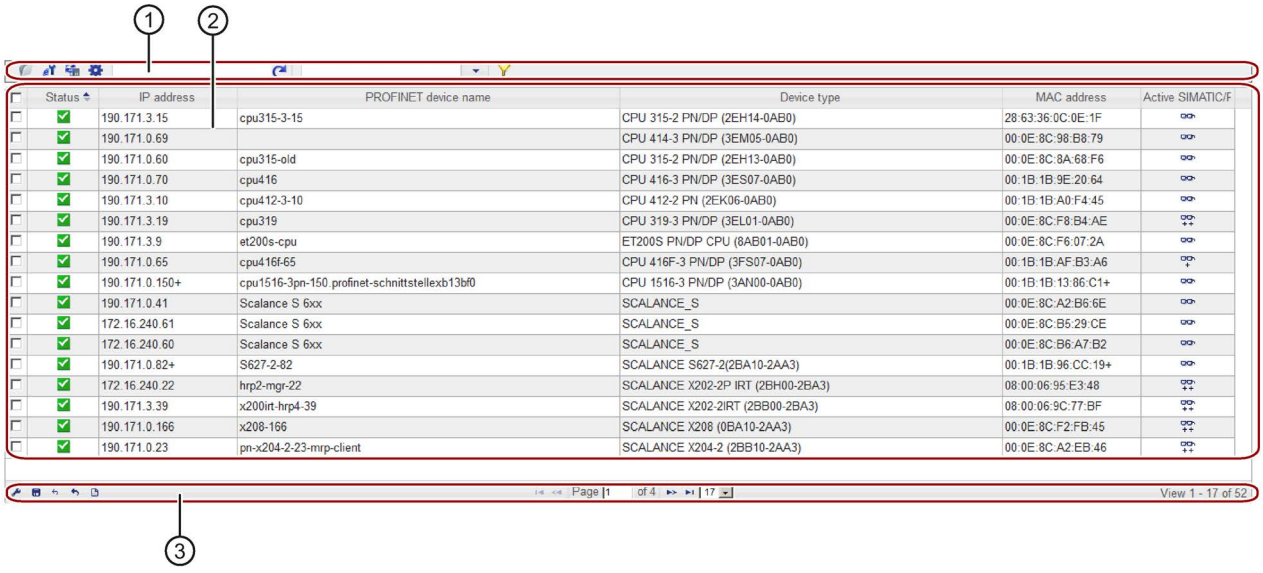
  The PROFINET IO system can be displayed with the aid of the information that the controller obtains from assigned PROFINET IO devices. To do this, the monitoring setting "SIMATIC monitoring of assigned devices" must be enabled for the controller. In a display of the PROFINET IO system initiated by the controller, the displayed IP addresses are always IP addresses reported by the controller. In this representation, devices are also displayed that are assigned to the controller but that are themselves not SINEMA Server objects.

- Other controller types:

  The PROFINET IO system can be displayed with the aid of information that PROFINET IO devices obtain from their controller. To do this, the monitoring setting "PROFINET monitoring" must be enabled for the PROFINET IO devices to be displayed. If the display of the PROFINET IO system was initiated by PROFINET IO devices, the tooltip of the associated entry displays "Discovered by: IO devices".

PROFINET IO devices that cannot be assigned are displayed under the entry "Unassigned devices".

4.1.7 Device window with device list



① Header with toolbar
② Device list with status display and configurable columns
③ Footer with setting functions and navigation

Display

You can open device lists of SINEMA Server by selecting an entry in the device tree. The "Devices" tab is always preselected in the device window.

Depending on the entry you select in the device tree, all devices or only a certain group are displayed in the device list.

Content

Device lists are divided into several columns in which the device-specific data is displayed. With the exception of the first column that is used to select rows, you can select any other column as required, see section User interface (Page 71). For example the column for IPv4 addresses displayed as default can be removed and the column for IPv6 addresses can be added. Values that can no longer be updated because protocol reachability is not available are displayed grayed out.

Possible monitoring statuses

The symbol in the "Active monitoring status" column specifies whether and what type of monitoring is active for a device. In the active monitoring status, the PROFINET/SIMATIC devices also include the globally and locally configured PROFINET/SIMATIC monitoring settings.

Icon	Meaning
	The device is not monitored.
	The PROFINET IO device becomes passive; in other words, only monitored by the CPU with SIMATIC capability assigned to the device. Passively monitored devices are shown only in the PNIO system they belong to. For passively monitored devices, no PROFINET monitoring settings can be configured. The passive monitoring of devices can be selected when the devices cannot be reached by SINEMA Server. Passively monitored devices do not require a device license. The requirement for passive monitoring is that the CPU with SIMATIC capability can be reached by SINEMA Server and that the monitoring setting "SIMATIC monitoring of assigned devices" is active for this CPU.
	The device is monitored by SINEMA Server with the aid of the protocols ICMP / DCP / SNMP.
	The device is monitored by SINEMA Server with the aid of the protocols ICMP / DCP / SNMP. Depending on whether a PROFINET IO device or a CPU with SIMATIC capability is involved, the following monitoring mode is also active: • PROFINET: The PROFINET monitoring of the PROFINET IO device by SINEMA Server is active. • SIMATIC: The SIMATIC monitoring of the CPU with SIMATIC capability by SINEMA Server is active.
	The device is monitored by SINEMA Server with the aid of the protocols ICMP / DCP / SNMP. Depending on whether a PROFINET IO device or a CPU with SIMATIC capability is involved, the following monitoring modes are also active: • PROFINET: – The PROFINET monitoring of the PROFINET IO device by SINEMA Server is active. – The PROFINET acquisition of port statistics of the PROFINET IO device by SINEMA Server is active. • SIMATIC: – The SIMATIC monitoring of the CPU with SIMATIC capability by SINEMA Server is active. – The SIMATIC monitoring of the PROFINET IO devices assigned to the controller by the CPU with SIMATIC capability is active. The SIMATIC monitoring of SIMATIC event / alarm messages is not shown in the displayed monitoring status.

Operator input

The following table shows the functional elements of the header.

Table 4- 3 Basic settings

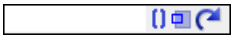
Icon	Display / function	Icon	Display / function
	Show details of the selected device		Call WBM (Web Based Management) If a Web page is available for the selected device, this is opened. This page displays specific information and settings for the selected network device.
	Reread device data The data of the device is read out again according to the active monitoring setting. Device data can be reread every 2 minutes.		Advanced settings Opens a menu bar in which the advanced settings are available. This is described in the table "Advanced settings", see below.
	Enter text to filter based on devices. The entered text is searched for in all columns. In the input box, text is displayed when a simple query entered in the filter template editor is active. The icon is displayed when a filter template with prefilter settings is active. The {} icon is displayed when a filter template with a complex query is active.		Selection of a previously created template for filtering according to devices. After selection, the properties of the filter template are applied to the device list. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
	Open the editor for configuring filter settings that can be stored in filter templates. The icon is displayed when the configured filter settings differ from the default filter settings. For more information, refer to the section "Prefilters in filter templates for device lists".		

Table 4- 4 Advanced settings

Icon	Display / function	Icon	Display / function
	Add or change comment		Delete remark
	Enable monitoring Enable monitoring for the selected devices. The PROFINET/SIMATIC monitoring that may be available for the device is performed according to the configured global and local PROFINET/SIMATIC monitoring settings. If the selected device is a PROFINET IO device and if the monitoring of assigned devices is activated for the controller assigned to it, as an alternative to activating monitoring by SINEMA Server, you can activate passive monitoring. In this mode, the PROFINET IO device is monitored only by the assigned CPU with SIMATIC capability.		Turn off monitoring Disable monitoring for the selected devices. If the selected device is a monitored PROFINET IO device and if the monitoring of assigned devices is activated for the controller assigned to it, as an alternative to fully disabling monitoring, you can also enable passive monitoring. In this mode, the PROFINET IO device is monitored only by the assigned CPU with SIMATIC capability.

Icon	Display / function	Icon	Display / function
	Change local monitoring settings The local PROFINET/SIMATIC monitoring settings functionally correspond to the global PROFINET/SIMATIC monitoring settings, refer to the section Administration - Monitoring General (Page 186). When SIMATIC monitoring is activated for a device, SNMP is used to check whether the device has a firmware version that has been released for SIMATIC monitoring by the SINEMA Server, refer to the section Administration - Monitoring General (Page 186). To activate SIMATIC monitoring for a device, this must therefore be reachable via SNMP and must have information about the installed firmware version. Local monitoring settings only take effect on devices when the global monitoring settings of the same name are active. Devices can also be configured as alternating devices. If the property "Alternating device" is removed from a device, all the connections learned for this device are deleted. The "SNMP Monitoring" check box is automatically disabled by SINEMA Server if the logon to the device fails with one of the configured SNMP settings to prevent the device from blocking the IP address of SINEMA Server. After you have corrected the respective SNMP setting under "Administration > Monitoring > SNMP settings", you can reactivate SNMP monitoring for the device via the "SNMP Monitoring" check box in the local monitoring settings.		Create new device Behavior when creating NAT devices: • SINEMA Server is located in the external subnet: The specified IP Address is the external IP address for the device at the NAT router • SINEMA Server is located in the internal subnet: The specified IP address is the IP address of the device.
	Delete device After it is deleted, the device only continues to exist in the report archive. When you delete a PROFINET IO device being monitored by a CPU with SIMATIC capability using the function "SIMATIC monitoring of assigned devices", this PROFINET IO device is discovered by the controller again after it has been deleted and therefore shown again in the corresponding PNIO system.		Specify SNMP settings

Icon	Display / function	Icon	Display / function
	Change device type Opens the "Set device type for" dialog in which a different device type can be assigned using the available profiles. DCP can also be enabled and the SNMP settings changed.		Change monitoring profile Opens the "Set monitoring profile for" dialog If necessary you can use this method to assign a monitoring profile to the device in addition to the general profile.
	Customize device data The "Adapt device" dialog opens. Here, you will find the following tabs for further entries: • User-defined links When necessary, you can store links (URL) to further information that is useful in conjunction with monitoring the device. • Basic data In this tab you can specify a device icon for the device, set the protocol and the port for calling the WBM and configure the article number of the device. The configuration of article numbers for several devices at the same time is possible only for devices that do not have a standard profile assigned to them. The article numbers configured by the user have a higher priority than article numbers detected by SINEMA Server.		Set device basic data

Prefilters in the filter templates for device lists

Device lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for device lists. You will find basic information on filter templates and the options of using complex filters in the section "Filtering data with filter templates" of the operating instructions of SINEMA Server.

Box group	Filter options
Basic filter	Filter according to devices for which the port statistics are activated /deactivated: • All • Yes: Devices with activated port statistics • No: Devices with deactivated port statistics Filter according to devices that are part / not part of the reference topology: • All • Yes: Devices that are part of the reference topology • No: Devices that are not part of the reference topology
Monitoring status	Filter according to devices with a certain monitoring status.

Functions of the shortcut menu

The functions presented above can also be called alternatively using the shortcut menu.

The shortcut menu also provides the option of calling up the topology display or a view-specific topology display from the device window. The device selected using the shortcut menu is shown centered and selected in the topology display.

Using the shortcut menu “Advanced settings” > Add new job”, you can create a new job for the selected devices. The selected devices are then automatically assigned to the job.

See also

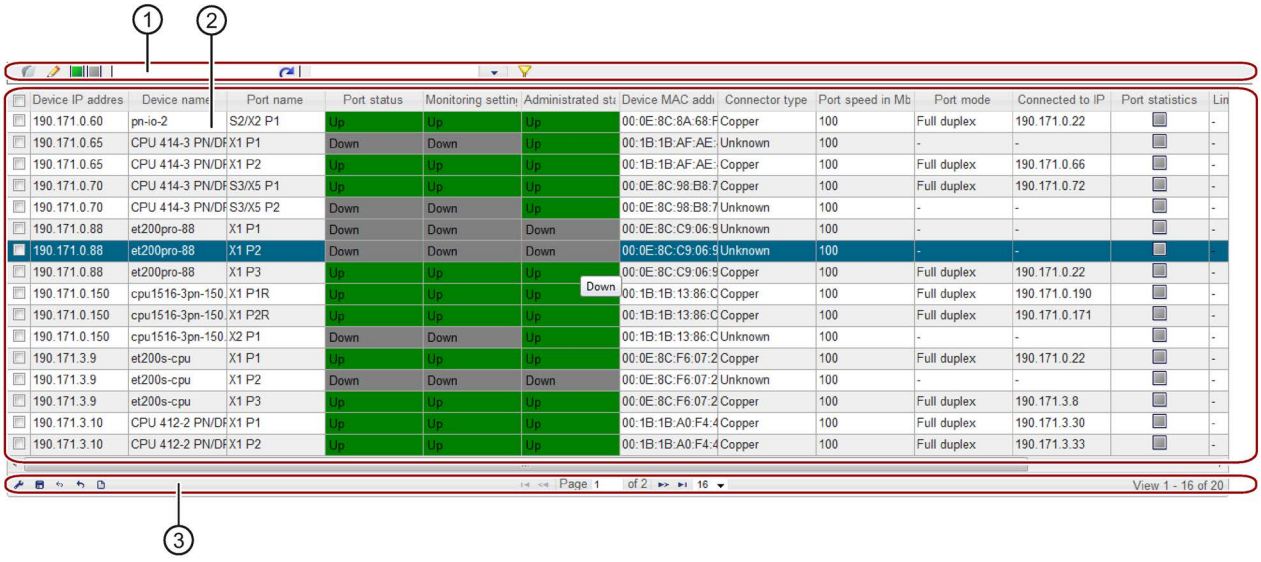
Filtering data with filter templates (Page 77)

Alternating devices (Page 120)

User interface (Page 71)

Device details (Page 104)

4.1.8 Device window with interface list



① Header with toolbar

② Interface list with configurable columns

③ Footer with setting functions and configuration limits (identical to the footer of the device list)

Display

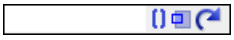
You can open interface lists of SINEMA Server by selecting an entry in the device tree. In the device window, then select the "Interfaces" tab.

Depending on the entry you select in the device tree, the interface list shows the interfaces of all devices or only the interfaces of a specific group of devices.

Operation / content

Interface lists are divided into several columns in which the data of the interfaces and their devices is displayed. With the exception of the first column that is used to select rows, you can select any other column as required.

The following table shows the functional elements of the header.

Icon	Display / function
	Show device details Depending on whether the selected interface is a LAN or WLAN interface, the "LAN" or the "WLAN" tab of the device details is opened.
	Edit port details The dialog for editing interface information opens. The meaning of the functions of this editor can be found in the section "Editor for detailed information on (W)LAN ports" in the operating instructions of SINEMA Server
	Enable / disable interface statistics. If the interface statistics are disabled, the interface is not included in reports that can be generated with "Reports > Availability > Interfaces".
	Enter text for filtering by interfaces. The entered text is searched for in all columns. In the input box, text is displayed when a simple query entered in the filter template editor is active. The icon is displayed when a filter template with prefilter settings is active. The {} icon is displayed when a filter template with a complex query is active.
	Selection of a previously created template for filtering according to interfaces. After selection, the properties of the filter template are applied to the interface list. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
	Open the editor for configuring filter settings that can be stored in filter templates. The icon is displayed when the configured filter settings differ from the default filter settings. For more information, refer to the section "Prefilters in filter templates for interface lists".

The shortcut menu provides the option of calling up the topology display or a view-specific topology display from the device window. The device of the interface selected using the shortcut menu is shown centered and selected in the topology display.

Prefilters in the filter templates for interface lists

Interface lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for interface lists. You will find basic information on filter templates and the options of using complex filters in the section "Filtering data with filter templates" of the operating instructions of SINEMA Server.

Operator control element	Filter options
From IP To IP	Filter according to interfaces that have the specified device IP addresses.
Device name and device type	Filter according to interfaces that belong to devices with the specified device name or device type.
Statistics activated	Filter according to interfaces for which the port statistics are activated /deactivated: • All • Yes: Interfaces with activated port statistics • No: Interfaces with deactivated port statistics

See also

Editor for detailed information on (W)LAN ports (Page 117)

Filtering data with filter templates (Page 77)

4.1.9 Device details

Display

You can call up the "Device details" window in the following ways:

- Device window
  - Symbol 
  - Double-click on the appropriate row
- Any topology view ("Topology > …" or "Views > …")
  - Shortcut menu of the device
  - Double-click on device icon

Overview

The "Device Details" window consists of several tabs in which the data from a device are grouped in a detailed manner or are displayed in list form.

Note

Tab display

Which tabs are displayed depends on the device type.

Operation / content

The following table shows the tab contents of the "Device Details" window with a brief explanation. For NAT devices the window title the external IP address is displayed in addition to the IP address and the name of of the device. The display scheme is: Internal IP address / external IP address / device name.

Only the tabs and boxes are displayed that are relevant to the selected device. The tabs and boxes relevant for a device whose content cannot be read out by SINEMA Server due to deactivated monitoring settings or the protocol currently being used are shown grayed out. Values that can no longer be updated because protocol reachability is not available are also displayed grayed out. In the "Expert" tab, you have the option of hiding such old values. In boxes whose values cannot be displayed despite available protocol reachability, the "-" character is displayed.

For newly discovered, passively monitored devices, only the "Overview" and "Events" tabs are displayed.

Table 4- 5 "Overview" tab

Parameter group	Display, content
-	Icon and overall status of the device. If the overall status is negative, the event that caused this overall status is also displayed.
Device name	IPv4 address, name, device category and type MAC address and location
NAT device identification	For devices that SINEMA Server can reach via NAT routers (1:1 NAT), instead of the parameter group "Device identification" the parameter group "Identification of NAT device" is displayed. The IP address and the MAC address of a NAT device are displayed in the boxes "Internal IP address" and "Internal MAC address". The detection of IP address changes is nor supported for NAT devices. The "External IP address" box displays the IP address configured on the NAT router for the device in the external subnet. SINEMA Server sends queries for monitoring the NAT device to this external IP address if SINEMA Server is not connected in the internal network. The "External MAC address" box displays the MAC address of the NAT router. For more detailed information on monitoring of NAT devices and NAT routers, refer to the section Monitoring of NAT devices and NAT routers (Page 122). For general information on NAT, refer to the Glossary.

Parameter group	Display, content
Pending events	Number of events pending for the device of the classes "Error", "Warning" and "Information"
Remarks	Comments, information

Table 4- 6 'Status' tab

Parameter group	Display, content
-	Overall status of the device. If the overall status is negative, the event that caused this overall status is also displayed.
Reachability	Information on the protocol-specific reachability of the device: Polling group, ICMP reachability ("Ping status"), SNMP reachability, overall status related to reachability, DCP reachability, SIMATIC or PROFINET reachability The overall status related to reachability is not influenced by DCP reachability.
Status details	In the "Device operational state" box, the device status obtained by SNMP is shown. For CPUs with SIMATIC capability, the Status LED and for PROFINET IO devices the PNIO Channel Status is shown. Notes on the LED status: • BUS1F: First bus error LED • BUS2F: Second bus error LED • BUS3F: Third bus error LED
Summary LAN ports	Number of ports in total, used, active and inactive (differing from reference), as well as with critical behavior
Times	Information, when • first and last time detected, • the last poll occurred, • the oldest stored data was read in and how long it was last active (up time)
Miscellaneous	Information relating to C-PLUG, power supply status

Table 4- 7 'Description' tab

Parameter group	Display, content
Names	PROFINET IO, system and automation name
Location	Location according to system and automation
Identification and maintenance	Article number, serial number, vendor ID and name, firmware version, hardware revision, DCP-ID
Manual changes	Information on whether the device type was changed and whether the device was migrated and created manually
User-defined links	Display of links 1 to 3, if entered You enter links using the "Customize device data" function.
Discovery and monitoring settings	Profile name and identifier, discovery and device type rule (in each case name and content), name and identifier of the monitoring profile

Parameter group	Display, content
Port assignment protocol	The "Port assignment" box displays whether or not the port-specific data of a device can be read out both using SNMP as well as using PROFINET and assigned to the corresponding ports. This is ensured when the data obtained via SNMP and PROFINET for the port assignment are compatible with each other. The port assignment allows SINEMA Server to switch over between SNMP and PROFINET depending on protocol availability. When there is such a protocol change, the following situations are distinguished: • All port information is compatible with the new protocol: The existing port information remains when there is a change of protocol. • Some port information is compatible with the new protocol: Only the information of the ports that can be read out and assigned via the new protocol are displayed. The information of the other ports is removed from the device details and from the topology. • No port information is compatible with the new protocol: The ports of the device are displayed grayed out in the device details and in the topology. In the "Protocol used" box, the protocol currently being used for reading out and for assigning port information is displayed. When using PROFINET, only the information of physical ports can be read out.
Miscellaneous	Contact, assigned filter groups for topology representation, OPC UA index, OPC DA index and information about the visibility in OPC

The "SIMATIC" tab is active for CPUs with SIMATIC capability with active SIMATIC monitoring. To detect multiple PROFINET IO systems on a CPU with SIMATIC capability, the SIMATIC monitoring of assigned devices must also be active.

Table 4- 8 'SIMATIC' tab (only active for CPUs with SIMATIC capability with active SIMATIC monitoring)

Parameter group	Display, content
SIMATIC identification	Information to identify the CPU with SIMATIC capability.
PROFINET IO controller	This area shows the interfaces of the CPU with SIMATIC capability at which it is configured as PROFINET IO controller.
Configured cycle time	Configured minimum and maximum value for the cycle time in ms.
Measured cycle time	The shortest, last read and longest cycle time read out by SINEMA Server in ms. The values for the cycle times are recalculated every 60 seconds.
SIMATIC status of assigned devices	This area shows how many of the assigned PROFINET IO devices have which status relating to the associated controller: • Configured devices: Total number of devices configured as PROFINET IO devices in STEP 7. • Active devices: Number of devices exchanging data with the controller. • Deactivated devices: Number of devices deactivated by the controller. • Faulty devices: Number of devices in the "Error" status. • Missing devices: Number of devices configured as PROFINET IO devices in STEP 7 that have, however, not been reached by the controller.

Parameter group	Display, content
SIMATIC event / alarm messages	Date and time of the last logon (to receive SIMATIC event and alarm messages from the CPU with SIMATIC capability): Time of the last attempted logon to the CPU with SIMATIC capability Date and time of the last read out: Time of the last successful read out of the display texts from the CPU with SIMATIC capability Date and time of the last attempted read out: Time of the last attempt to read out the display texts from the CPU with SIMATIC capability
H-system	For SIMATIC S7-400-H CPUs, the operating mode of the associated H system (redundancy mode / stand-alone mode) as well as the operating mode of the modules involved (RUN / STOP) are displayed in this area. It is also specified which CPU is currently in master mode and which in standby mode. The CPU whose device details are open is highlighted in blue. Double-click the partner CPU to call up its device details. To display both CPUs of the H system, SIMATIC monitoring must be activated for both CPUs.

Table 4- 9 'PROFINET' tab (only active for PROFINET IO devices with active PROFINET monitoring)

Parameter group	Display, content
PROFINET identification	Information to identify and to assign the controller of the PROFINET IO device
High Availability	For devices with High Availability support, the High Availability operating mode (redundancy mode / stand-alone mode) is displayed in this area. The "HA device diagnostics" table shows the detected PROFINET interface modules of the device and the assigned controllers. SINEMA Server treats each PROFINET interface module of an HA device as a separate device. The PROFINET interface module whose device details are open is highlighted in blue. Double-click the partner module to call up its device details.
PROFINET diagnostics	PROFINET standard diagnostics contains status information of the PROFINET IO device at the slot and subslot level. This, for example, informs you about configured modules that do not exist in slots. PROFINET channel diagnostics collects additional status information from channels. With the "Diagnostics details" button, a table can be called which displays additional diagnostics details such as the weighting (Severity) of negative statuses. In the "Text" column of the PROFINET standard diagnostics and the PROFINET channel diagnostics, the texts of the PROFINET diagnostics library are shown that could be assigned to the read out raw data of the devices. If no assignment could be made the raw data is displayed in hexadecimal format. For more information on the diagnostics texts, refer to section Administration - Monitoring General (Page 186). Only current data is displayed, historical data is displayed only in corresponding events.

Table 4- 10 'Config.' tab (Configuration)

Parameter group	Display, content
Ethernet	MAC address of the device
IP addresses	Display of the IPv4 and IPv6 addresses of the device with standard gateway, subnet mask and origin of the IP addresses, e.g. assignment via DHCP.

Parameter group	Display, content
PROFINET	PNIO name and type
SNMP settings	Configuration name, traps enabled, SINEMA Server trap recipient (yes / no)
General SNMP traps	Information about whether the following traps were enabled: • Connection establishment and termination • Warm and cold restart • Authentication failed
Miscellaneous	Radius server address; IP forwarding (yes / no / not supported) Alternating device (yes / no)

Table 4- 11 'LAN' tab

Parameter group	Display, content
-	Table of all LAN ports with designation, status, MAC address, connection type, speed and other freely selectable information. The entire table can be formatted and used as described for the device window (column width, export etc.). There are icons available above the table with following functions: • Show port details • Change port details, refer to the section "Editor for detailed information on (W)LAN ports" in the operating instructions of SINEMA Server • Enable port statistics • Disable port statistics If statistics is activated for a port, information about data traffic, port load and error rates is monitored using SNMP or possibly PROFINET.

Table 4- 12 'WLAN' tab

Parameter group	Display, content
-	Table of all WLAN interfaces with index, name, status, SSID and information about critical statuses. The content of the table corresponds to the "LAN ports" tab. The "Open interface" icon provides you with more detailed information.

Table 4- 13 'Events' tab

Parameter group	Display, content
-	Table of all reported events with name, status, timestamp, status and other arbitrary information. The entire table can be formatted and used as described for the device window (column width, export etc.). There are icons available above the table with following functions: • Mark events as "Read" • Resolve pending events • Add / edit remark • Delete remark • Filter options similar to event list

Table 4- 14 "IP Interfaces" tab

Parameter group	Display, content
-	Display of all interfaces of a device with relevant IPv4 or IPv6 address and the associated connection status. The table is displayed only for devices that can be reached via at least two IP addresses. For NAT routers of the module type SCALANCE S in addition to the IP addresses of the interfaces, the IP addresses are displayed via which SINEMA Server can reach NAT devices with 1:1 NAT. With the square button at the top left edge, the interface can be specified whose IP address will be used to monitor the device. For interfaces with IPv6 addresses and for external IP addresses of NAT devices this is not possible.

Depending the NAT router being used, the "NAT" tab displays the configurations for static NAT (1:1 NAT), Pooled NAT and NAPT. The NAT rules are displayed regardless of whether NAT was enabled for the NAT router. The displayed NAT rules can contain IPv4 or IPv6 addresses.

You will find information on the supported NAT routers in the section Monitoring of NAT devices and NAT routers (Page 122).

For general information on NAT, refer to the Glossary.

Table 4- 15 "NAT" tab

Tab	Display, content
Static NAT (1:1 NAT)	NAT rules for static NAT (1:1 NAT)
Pooled NAT	NAT pools of the NAT router with external start and end addresses. A maximum of 20 NAT pools can be displayed. After double-clicking on a NAT pool the NAT devices are displayed that use the particular NAT pool.
NAPT	NAPT rules for IP address translations with port forwarding.

Table 4- 16 'VLAN' tab

Parameter group	Display, content
Basic data	Maximum number of possible VLANs and currently used VLANs
VLANs	Table of the currently used VLANs with identifier (VID), name and status and the "tagged" and "untagged" ports.

Table 4- 17 'Redundancy' tab

Parameter group	Display, content
-	Table of all redundancy mechanisms used with the ports involved, protocol used, status, role (manager or client) along with supplementary information. The "Open port details" icon provides you with incoming information.

Table 4- 18 'Expert' tab

Parameter group	Display, content
-	Listing of all the parameters read from the device with associated value, protocol and time of the last change on the device. The values of this tab are made available as raw data and are not further prepared. The data is therefore primarily for analysis by experts, for example by product support. In the box above the table, you can enter a search text that has the effect of a filter criterion for all columns of the table. Using the drop-down list, you can restrict the display to one of the protocols used to read out. If the value "All" is selected in the drop-down list and you enable the check box "Do not display value if not reachable via protocol", parameters whose values can no longer be read out via the relevant protocol are shown grayed out. If one of the protocols is selected in the drop-down list, values that can no longer be read out are hidden.

Table 4- 19 'User-defined OIDs' tab

Parameter group	Display, content
-	Table of MIB objects (see "Expert" tab) that are monitored as result of individual user settings.

Note

Display of the OID values

The correctness of the display of the OID depends on the correct selection of the data type in the profile setting.

Functions of the shortcut menu

The following functions are available in all tabs via the shortcut menu:

- Open WBM
- Reread data

  For more detailed information, refer to section Device window with device list (Page 96)
- Enable/disable automatic update
- Add current window to quick links
- Log on again for SIMATIC event / alarm messages (with active SIMATIC monitoring in SIMATIC tab)

  For more detailed information, refer to section Administration - Monitoring General (Page 186)
- Open help
- Display selected device in the (view-specific) topology (only available for devices monitored by SINEMA Server)

See also

Detailed information WLAN (Page 116)

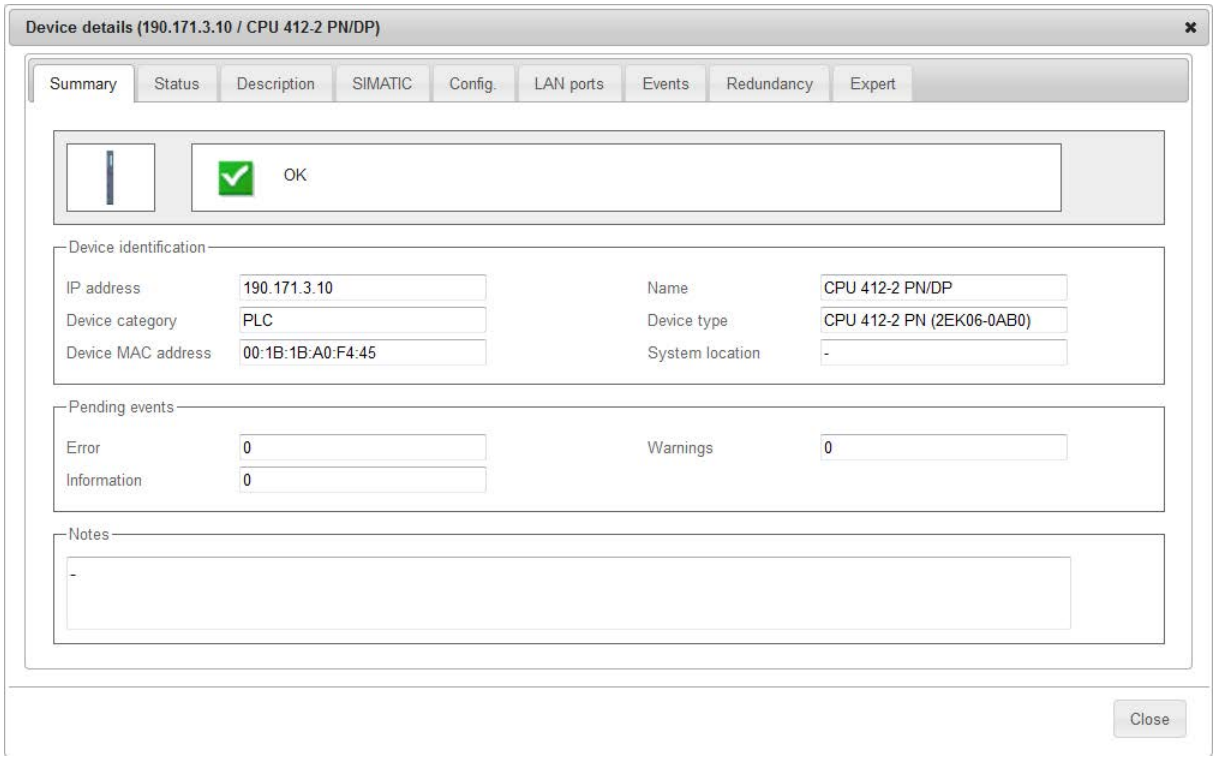
Editor for detailed information on (W)LAN ports (Page 117)

Alternating devices (Page 120)

Glossary (Page 295)

Event list (Page 128)

The following figure shows the "Overview" tab of the device details as an example of the tabs available.



4.1.10 Device details - subcategories

4.1.10.1 Detailed information LAN ports

Opening the display

You can open the "LAN ports" window from the "LAN ports" tab of the device details as follows:

- Select the port and then click the icon
- Double-click on the appropriate row

Operation / content

The following table explains the groups and contents of the box.

The values of the box groups “Data traffic", “Utilization" and “Error" are only monitored if port statistics is activated. All static values are delta values that are called every 5 minutes. The following symbols indicate the communication directions of the corresponding data values:

Icon	Communication direction
	Send
	Receive
	Half duplex (sending or receiving)

Group	Display, content
Basic data	• Name of the connector (detected) • SNMP interface index (unique number of the connection) • Port MAC address • Connector type (user-defined) • Connection type (detected) • Status (up or down) • Admin status • Max. bandwidth (Mbps) • Port mode (full duplex or half duplex) • Description • Alias name
Topology	• Device connection (IP address, device name) • Port connection If a reference topology exists, the values in this section originate from the reference topology. If no reference topology exists, the values in this section originate from the discovered topology information.
Discovered topology	• Device connection (IP address, device name) • Port connection
Plastic Optical Fiber (POF)	• Signal delay (ns) • Calculated cable length (m), according to the calculation in STEP 7 • Power budget
Data traffic	• Transmit (transmission speed in Mbps) • Receive (receive speed in Mbps)
Utilization	Full duplex: • Transmit utilization (degree of utilization as a percentage) • Receive utilization (degree of utilization as a percentage)
	Half duplex: • HD utilization (combined degree of utilization as percentage)

Group	Display, content
Error	Full duplex: • Transmit error rate (error rate as a percentage) • Receive error rate (error rate as a percentage) • Number of send errors (number of bad outgoing packets) • Number of receive errors (number of bad incoming packets) • Number of discarded outgoing packets • Number of discarded incoming packets
	Half duplex: • HD error rate (combined error rate as percentage) • Number of errors (combined a number of bad packets) • Number of discarded packets (combined number of discarded packets)
Statistics	Time at which port statistics was enabled for the selected port.

4.1.10.2 Detailed information WLAN

Opening the display

You can open the details window for WLAN interfaces from the "WLAN" tab of the device details as follows:

- Select the port and then click the icon
- Double-click on the appropriate row

Operation / content

The following table explains the groups and contents of the box. All static values are delta values that are called every 5 minutes.

Group	Display, content
Basic data	• Name of the connector (detected) • Description • Interface index (unique number of the port) • Authentication type (e.g. WEP or WPA2-PSK) • SSID (names of the WLANs (wireless networks) assigned to the interface) • BSSID (ID numbers of the WLANs assigned to the interface) • WLAN protocol (wireless standard acc. to IEEE: e.g. 802.11n or 802.11g) • Channel (wireless channel of the interface) • Frequency (wireless frequency of the interface) • Max. data rate (Mbps) • Mode (full duplex or half duplex)
Status	• Status (up or down) • Signal strength (strength of the wireless signal in dBm) • Transmit data rate (transmit speed in Mbps) • Receive data rate (receive speed in Mbps) • Transmit error rate (error rate as a percentage with more than 10 errors in the last 5 minutes) • Receive error rate (error rate as a percentage with more than 10 errors in the last 5 minutes) • Faulty, sent packets (in the last 5 minutes) • Faulty, received packets (in the last 5 minutes) • Number of clients (number of clients connected via this interface)

Group	Display, content
Clients	Table of all clients connected to the interface. Per client, the following information can be displayed: • Slot number (number of the connected interface) • Client name • Client IP (IP address of the connected client) • Client MAC (MAC address of the connected client) • Transmit data rate (transmit speed in Mbps) • Receive data rate (receive speed in Mbps) • Transmit error rate (error rate as a percentage with more than 10 errors in the last 5 minutes) • Receive error rate (error rate as a percentage with more than 10 errors in the last 5 minutes) • Critical performance (information as to whether or not the existing connection needs to be considered critical) • Signal (signal strength of the existing connection in dBm) • Signal state (indicates whether the signal strength is OK, low or high)

4.1.10.3 Editor for detailed information on (W)LAN ports

Opening the editor

You can call up the dialog for editing port information from the "LAN" and "WLAN" tab of the device details as follows:

Select the port and then click the  icon.

Operation / content

The following tables explain the contents of the box.

Table 4- 20 Basic data (only for LAN ports)

Parameter	Meaning
Connector type	Display of the connector type detected by SINEMA Server
Connector type (user-defined)	Selection of the connector type

Table 4- 21 Port monitoring

Parameter	Meaning
Unmonitored port (only for LAN ports)	If this option is selected, the port is handled as follows: • Port connection statuses are not monitored • Events relating to port reference statuses are not displayed If this option is disabled, all reference connections of this port are deleted.
Docking port (only for LAN ports)	If this option is selected, the port is handled as follows: • Port connection statuses are not monitored • Events relating to port reference statuses are not displayed • Connections of this port are learned when in "Administration > Monitoring > General" the check box "Learn connections of alternating devices automatically" is enabled. If this option is disabled, learned connections for this port and the corresponding reference connections of this port are deleted.

When a reference connection goes out from an interface, this cannot be configured as "Down".

See also

Alternating devices (Page 120)

4.1.10.4 Detailed information redundant ports

Opening the display

Alternatively the window with details for redundant connectors can be opened from the "Redundancy" tab of the device details as follows:

- Select the port and then click the icon
- Double-click on the appropriate row

Operation / content

Depending on the redundancy method (protocol) being used, different information is displayed. With the help of PROFINET monitoring, only MRP redundancy information can be displayed. The following table shows the possible content with a brief explanation.

Protocol	Group	Display, content
HRP	Basic data	• Port name (e.g. X5P1) • Role (what is the task (client, master) of the interface within the ring?) • Port status (information about what the interface does with IP packets . forward or block)
	Redundancy manager	• Ring state (OK, disrupted) • Ring state changes (number of status changes already made due to disruptions in the ring) • Measured trip delay (indicates in ms how quickly the status change is made)
MRP	Basic data	• Name of the port (e.g. X5P2) • Role (what is the task (client, master) of the interface within the ring?) • Port state (information about what the interface does with IP packets . forward or block. Is only displayed via SNMP) • Domain name
	Redundancy manager	• Ring state (OK, disrupted) • Ring state changes (number of status changes already made due to disruptions in the ring. Is only displayed via SNMP) • Measured trip delay (indicates in ms how quickly the status change is made. Is only displayed via SNMP) • Time ticks since (Is only displayed via SNMP) • Domain error (Is only displayed via SNMP)

Protocol	Group	Display, content
STP or RSTP	Basic data	• Name of the port (e.g. X0P5) • Connector type • Port STP state • Port status • Path costs (notional calculated costs for the current transport path of the IP packets). Path costs are used to calculate the most suitable transmission path.) • Priority • No .´Forward transmissions´ • Big network support • Passive Listening
Standby	Basic data	• Name of the port (e.g. X6P1) • Role (what is the task (master, master) of the interface on the "duplicate" connection?) • Port state (information about what the interface does with IP packets . forward or block) • Connection status (up, down) • Topology changes (number of topology changes already made due to disruptions on the connection) • Connection name (name of the standby connection. Required for identification since several may exist).

4.1.11 Alternating devices

Meaning

An alternating device is a device that is deliberately not permanently connected to the network.

Alternating devices can, for example, be engineering PCs that are only connected for diagnostics. Alternating devices also occur when using tool changer devices. The PROFINET IO devices connected to tool changer devices are switched active or inactive as necessary. In both cases, alternating devices are only reachable temporarily for SINEMA Server.

Handling of alternating devices in SINEMA Server

If alternating devices cannot be reached by SINEMA Server, it is assumed that they have been deliberately deactivated or are not connected to the network. For this reason, the devices do not receive the overall status "Not reachable" but rather "Not connected". No reachability related events are displayed for devices in the "Not connected" status. As soon as the devices can be reached again, the device overall statuses and the reachability-related events are displayed normally again.

Devices can be recognized as alternating devices automatically if they support the "Fast startup" function and when the corresponding check box has been enabled in SINEMA Server, see section Administration - Monitoring General (Page 186).

As an alternative, devices can be configured manually in the monitoring settings as alternating devices, refer to the section Device window with device list (Page 96).

Connections from alternating devices to tool changer devices, can be learned by SINEMA Server and displayed in addition to the current connection in the topology displays. Learned connections remain displayed in SINEMA Server after they have been terminated. For more information, refer to section Administration - Monitoring General (Page 186).

Note

PROFINET IO devices configured as alternating

With PROFINET IO devices that are not reachable by SINEMA Server and that are monitored by controllers using the function "SIMATIC monitoring of assigned devices", the SIMATIC status reported by the corresponding controller decides the overall status of the device. If the controller reports the PROFINET IO device as being deactivated, the IO device has the overall status "Not connected". If the controller does not report the PROFINET IO device as being deactivated, the IO device has another overall status. This applies regardless of whether the PROFINET IO device is configured as alternating.

Note

Events pending for alternating devices

Events that were triggered for a device are still pending for this device even after it is configured as an alternating device and are not resolved automatically. Such events need to be resolved manually.

See also

Editor for detailed information on (W)LAN ports (Page 117)

4.1.12 Monitoring of NAT devices and NAT routers

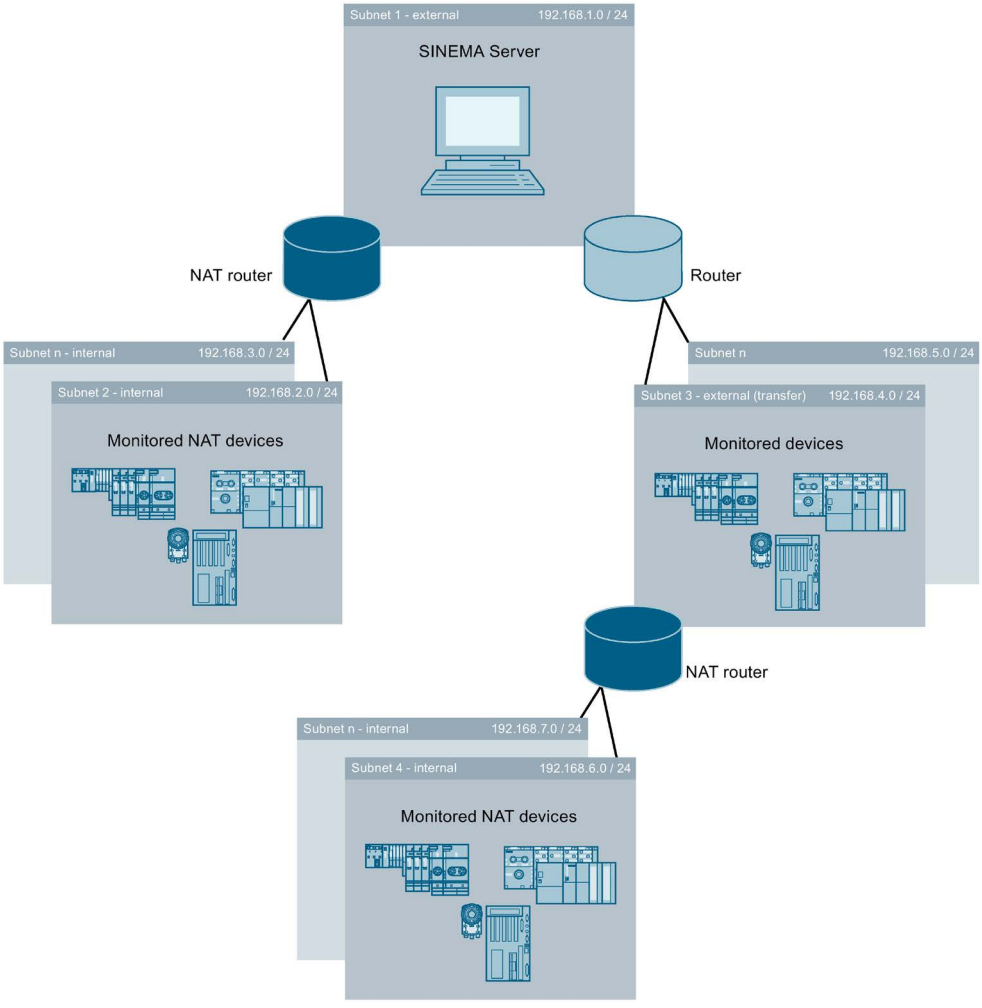
SINEMA Server supports the monitoring of devices that can be reached via NAT routers. In addition to this SINEMA Server shows NAT configurations of NAT routers. For a device separated from SINEMA Server by a NAT router the term "NAT device" is used below.. For the discovery of NAT routers and NAT devices during the network scan, the check box "Additional discovery of NAT routers during network scan" must be activated in "Administration > Discovery > Scan".

For general information on NAT, refer to the Glossary.

The monitoring of NAT devices and NAT routers by SINEMA Server is possible in the following network constellations.

Supported network constellations

SINEMA Server can be located in an external subnet and monitor devices of internal subnets that are connected to the external subnet via a NAT router, As an alternative SINEMA Server can be separated from the external subnet by routers. In special applications (e.g. series machines) the individual internal subnets can be configured identically (same subnet mask and IP addresses).



Even when SINEMA Server is located in one of the internal subnets, the devices of this subnet can be monitored. Devices can be recognized as NAT devices when the NAT router supports the NATv2-MIB (RFC7659). If the NAT router does not support this MIB, the devices are not recognized as NAT devices. The NAT procedures described below assume that SINEMA Server access to the NAT devices is via the external subnet.

Supported NAT procedures

SINEMA Server can monitor NAT devices that can be reached via static NAT (1:1 NAT). For each NAT device to be monitored there must be a separate IP address configured on the NAT router to which the SINEMA server can send queries for monitoring the NAT device. The NAT router forwards the monitoring queries to the IP address of the NAT device in the corresponding internal subnet. 1:1 NAT rules configured for NAT routers are displayed in the device details of SINEMA Server in "NAT > Static NAT (1:1 NAT)".

NAT pools from which IP addresses are selected dynamically and used as new source IP addresses of IP packets are displayed in the device details of NAT routers in "NAT > Pooled NAT". After double-clicking on a NAT pool the NAT devices are displayed that use the particular NAT pool. NAT devices with dynamic address assignment cannot be monitored by SINEMA Server.

NAPT rules based on which a NAT router not only translates IP addresses but also TCP/UDP ports are shown in the device details in "NAT > NAPT". NAT devices that can be reached via NAPT rules cannot be monitored by SINEMA Server.

The NAT router configurations displayed in the "NAT" tab can contain IPv4 or IPv6 addresses.

Supported NAT routers

NAT router	SNMP is enabled for NAT devices	NAT device details "Identification of NAT device" are available (1:1 NAT)	NAT router configurations are available in device details		
			Static NAT (1:1 NAT)	Pooled NAT	NAPT
NAT routers with support for MIB NATv2 (RFC 7659), e.g. SCALANCE S615 V5.0 or higher, SCALANCE SC-600 V2.0 or higher, SCALANCE XM-400 / XR-500 V6.1 or higher	Yes	Yes	Yes	Yes	Yes
	No	As long as made available via NAT routers	Yes	Yes	Yes
SCALANCE S602	Yes	Yes *	Yes	No	No
SCALANCE S612 SCALANCE S613 SCALANCE S623 SCALANCE S627-2M	No	As long as made available via NAT routers	Yes	No	No
NAT routers without support of the MIB NATv2 (RFC 7659) (no SCALANCE S)	Yes	Yes	No	No	No
	No	No	No	No	No

* If SINEMA Server is operated in the internal subnet, devices located in the same subnet are not displayed as NAT devices.

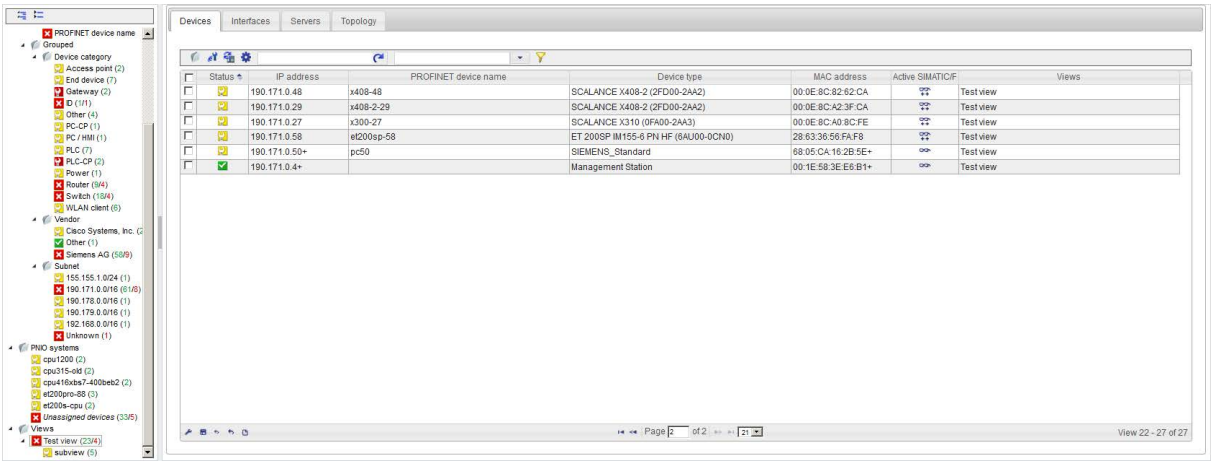
See also

Glossary (Page 295)

4.1.13 Views

4.1.13.1 Views - Overview

The following figure shows the layout and operator controls of the "Views" window, "Devices" tab.



Opening a view

You can open the "Views" window of SINEMA Server by selecting the entry with this name in the device tree or one of its lower-level entries.

The "Devices", Interfaces" and "Servers" tabs are always present, the "Topology" tab only if this has been configured accordingly (selected).

Working with and content of the "Devices" tab

The "Devices" tab displays the devices that were assigned to the selected view with the View editor. As default, the device list of a view also includes the "Views" column. This column shows the views in which the device occurs.

See also

Device window with device list (Page 96)

Setting up and using views (Page 61)

Working with and content of the "Interfaces" tab

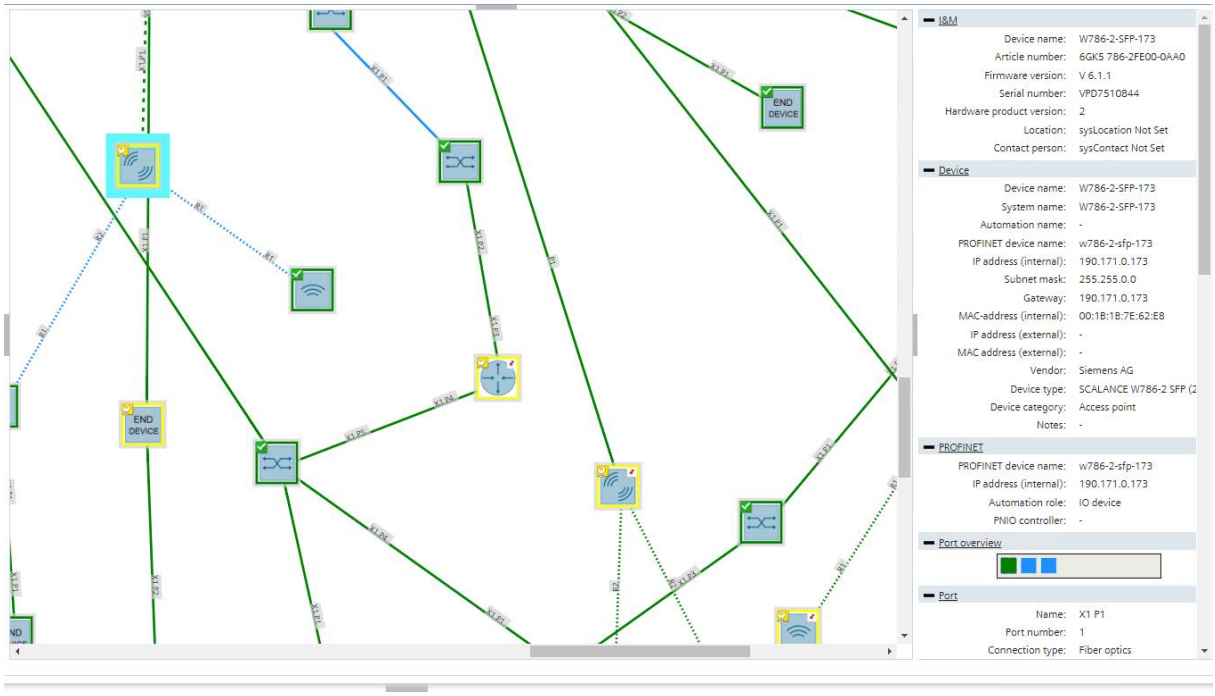
The "Interfaces" tab displays information about the interfaces of devices that were assigned to the selected view with the View editor. There is no difference compared with the interface list that is not dependent on the view.

Working with and content of the "Servers" tab

The "Servers" tab shows SINEMA Server instances that were created in the server overview and assigned to the current view. In the server list of a view, the columns for displaying the overall device status are not available. Similar to the "Devices" tab, the "Views" column shows the names of the views to which the SINEMA Server instances are assigned.

4.1.13.2 Views . topology

The following figure shows the layout and operator controls of the "Views" window, "Topology" tab in Online mode.



To configure and display view-specific topologies a reference topology must already have been created and saved. Devices must be part of the reference topology to be able to be inserted in view-specific topologies.

Topology modes

Initially in the editing mode the reference devices, sub views, SINEMA Server instances contained in the view and the unmanaged devices existing in the reference topology in the left page area "User-defined view" can be dragged and positioned in the topology display. Between monitored devices and unmanaged devices, the configured reference connections are shown. Between the inserted elements, you can draw in user-defined connections manually or adopt existing reference connections as user-defined connections. SINEMA Server instances can only have manually drawn, user-defined connections to other SINEMA Server instances. On user-defined connections with the shortcut menu bending points can be generated with which the course of user-defined connections can be adapted. For more information, refer to section "Operator input".

In Online mode the elements inserted in Editing mode with their monitoring statuses for devices and ports and the user-defined connections drawn between them are displayed. Reference connections are not displayed in Online mode.

The colors of devices, ports and user-defined connections have largely the same meaning and formation rules as the colors of the non-specific view topology.
There are the following special features in the Editing mode of view-specific topologies:

- Reference connections are displayed in violet.
- User-defined connections are displayed in black.
- If both connection types apply, the connection color is shown in violet and black.

There are the following special features in the Online mode of view-specific topologies:

- For user-defined connections the connection color is decided by the fill color of the ports involved.
- Deviations between user-defined connections and discovered connections are not indicated in view-specific topologies.

The following applies to the display of SINEMA Server instances:

- The reachability status of the SINEMA Server instance is indicated by a colored line at the lower edge of the object. The meaning of the colors for the instance symbol corresponds to the meaning of the colors for the SINEMA Server monitor symbol.
- In the top left corner of the object, you can see the most negative overall device status of the SINEMA Server instance.
- User-defined connections between two SINEMA Server instances are always shown in gray.

Operator input

Operation is largely identical to the operation in the non-view-specific topology. Functions used for the configuration of the reference topology are not available in view-specific topologies. The reference statuses of ports can therefore not be configured. Below the operator input elements of the toolbar are explained in greater detail. For the differences to the non-view-specific topology, refer to the section Topology (Page 134).

Symbol	Display / function	Icon	Display / function
	Topology settings The settings that are saved for each user for view-independent topologies are saved for each specific view here.		Selection tool Bending points cannot be inserted for reference connections but for user-defined connectioons.
	Drawing tool With the drawing tool, user-defined connections can be drawn manually. SINEMA Server instances can only have connections to other SINEMA Server instances.		Showing reference connections The reference connections created in the non-view-specific topology are displayed.
	Adopt reference connections as user-defined connections Creates user-defined connections for all reference connections Individual reference connections can be adopted as user-defined connections with the shortcut menu or by double-clicking.		

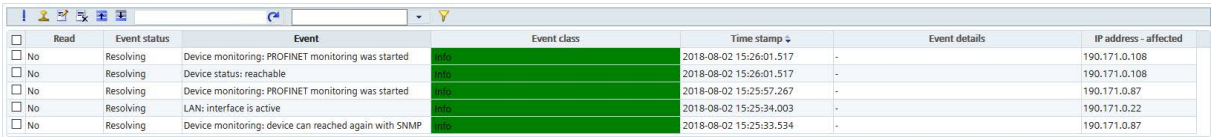
See also

Status display (Page 30)

4.1.14 Event list

Event list

The event list shows all the events in the form of a table. This page provides various navigation options in the upper part of the page. For each event, specific parameters are displayed in a separate table row that are explained below.



Read	Event status	Event	Event class	Time stamp	Event details	IP address - affected
No	Resolving	Device monitoring: PROFINET monitoring was started	Info	2018-08-02 15:26:01.517	-	190.171.0.108
No	Resolving	Device status: reachable	Info	2018-08-02 15:26:01.517	-	190.171.0.108
No	Resolving	Device monitoring: PROFINET monitoring was started	Info	2018-08-02 15:25:57.267	-	190.171.0.87
No	Resolving	LAN: interface is active	Info	2018-08-02 15:25:34.003	-	190.171.0.22
No	Resolving	Device monitoring: device can reached again with SNMP	Info	2018-08-02 15:25:33.534	-	190.171.0.87

Extent of the display - user management and views

Which events are displayed also depends on the views assigned to the currently entered user. This means that events are only monitored if they are associated with the configured views.

Meaning

Below you will find information about the significance of the individual boxes:

Column	Meaning
"Check box"	The selection box is used to select an event prior to editing a particular event. Multiple selections are possible. Note: By double-clicking on the selected event you open the device details ("Events" tab) of the device belonging to the event.
Read	Display indicating whether the event was read by the user with the "Events read" function. • "Yes" = Read • "No" = Not read
Event status	Display of the status that the event has in terms of the overall status of a device or of the overall status of SINEMA Server. • Pending: When an event that is assigned a negative overall status (every overall status except "OK" and "Not connected") is triggered for a device / SINEMA Server, it is given the event status "Pending". This status indicates that the event was entered in a list of pending events for the device / SINEMA Server. • Resolved automatically: An event was removed from the list of pending events is identified by the event status "Resolved automatically". Resolved events can no longer influence the overall status of devices / SINEMA Server. Pending events are automatically resolved by the following events: – Events assigned the "OK" or "Not connected" overall status from the same overall status group – Pending events of the same overall status group (regardless of the assigned overall status) • Resolved manually: A pending event that was removed from the list of pending events manually using the stamp icon in the event list is identified by the event status "Resolved manually". • Not present: A triggered event that is not assigned to any overall status group or is not assigned any overall status in the group has no event status.
Event	Configured event information or event message.

Column	Meaning
Event class	Information on the class (weighting) of the event. The entries are color-coded with the following meaning: • light green = notification • dark green = information • yellow = warning • red = error
Time stamp	The "Time stamp" box provides information on the date and time of the generation of the event.
Event details	Shows the full information for each event.
IP address (affected)	Shows the IP address of the device that triggered the event.
IP address (reporting)	Shows the IP address of the device that reported the information to trigger the event to SINEMA Server.
External IP address (affected)	Shows the IP address of the NAT router for the device that triggered the event.
External IP address (reporting)	Shows the IP address of the NAT router for the device that reported the information to trigger the event to SINEMA Server.
Remarks	Store additional information, for example, about event reactions. Note: If several events are selected, an edited comment is entered for all the selected events.
Trigger	Name of the source device.
Time stamp (reported)	Time at which the SIMATIC event / alarm message was sent by the CPU with SIMATIC capability.
Event category	Specifies whether a network event or a system event is involved.
Device status	Overall status that potentially causes the event on a device / SINEMA Server.
Overall status group	Name of the overall status group to which the event is assigned.
Affected (name)	Shows the PROFINET name of the device that triggered the event.
Reporting (name)	Shows the PROFINET name of the device that reported the information to trigger the event to SINEMA Server.
Protocol	Information about which protocol supplied the event information.
Interface / slot	Provides information on the interface type being used and the interface number or on the slot, subslot and channel of the PROFINET device.

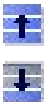
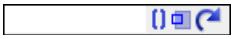
Note

Receiving SNMP traps

SINEMA Server receives SNMP traps only if the IP address of the SINEMA Server is configured on the relevant devices as the trap destination.

Operator input

The following table explains the function elements of the header.

Icon	Meaning
	Events read By marking events as "Read", you confirm your awareness of the changed status of an active entry in the event list. No other reaction is associated with this function. Configured event reactions are triggered solely by the status change of the event.
	Removes a selected pending event from the list of events pending for a device. The event then has the event status "Manually resolved".
	Edit remark Note: If several events are selected, an edited comment is entered for all the selected events.
	Delete remark
	Maximize / minimize As default, SINEMA Server shows up to 10 events in the event list. By maximizing the display, you expand the display of the event list to the size of the full Web page. Using the functions in the footer, you also have the option of paging through the entire event list and configuring the layout of the event list.
	Enter text to filter based on events. The entered text is searched for in all columns In the input box, text is displayed when a simple query entered in the filter template editor is active. The icon is displayed when a filter template with prefilter settings is active. The {} icon is displayed when a filter template with a complex query is active.
	Selection of a previously created template for filtering according to events. After selection, the properties of the filter template are applied to the event list. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.

Icon	Meaning
	Open the editor for configuring filter settings that can be stored in filter templates. The  icon is displayed when the configured filter settings differ from the default filter settings. For more information, refer to the section "Prefilters in filter templates for event lists".
	Not connected / connected to topology If the topology display is shown in the content area, you have the option of connecting the event list to this topology display. In the connected status, devices for which events of the event list were triggered are highlighted optically in the selected topology representation. The devices whose events are highlighted can be specified in the "Highlight only selected entries" check box: • Check box is enabled: Only the devices of the events selected in the event list are optically highlighted. • Check box is disabled: All devices of the current event list are optically highlighted. Using the filter settings of the event list, the number of highlighted devices can be adapted. The highlighted devices are listed in the left side area. If the automatic updating is disabled, you can call up the highlighted devices one after the other with the shortcut menu in the topology display. The order in which they are called is based on the listing of the highlighted devices in the left side area.

Prefilters in the filter templates for event lists

Event lists can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for event lists. You will find basic information on filter templates and the options of using complex filters in the section:
Filtering data with filter templates (Page 77)

Box group	Filter options
Basic filter settings	Read: • Yes • No • All Event state: • All • " - " • Resolved automatically • Resolved manually • Pending Period: Filter according to events • the last X hours • the last X days • of a manually entered time range X: Number specified by the user
Event categories	Filter according to the origin of events: • Network events • System events
Event classes	Filter according to the severity of events: • Notification • Information • Warning • Error
Protocols	Filter according to protocols by which the events were triggered: • ICMP • DCP • ARP • SNMP • SNMP trap • PROFINET • SIMATIC • Multiple (event was triggered by more than one protocol) • SIMATIC event messages • SIMATIC alarm messages

Functions of the shortcut menu

The shortcut menu provides the option of calling up the topology display or a view-specific topology display from the event list. In the topology display, the device is selected and shown centered that triggered the event selected in the event list. This function is not available for traps that SINEMA Server has received from unknown devices.

In addition to this, you can call the overall status group to which the selected event belongs using the shortcut menu.

See also

Administration - Events > Event reactions (Page 205)

4.2 Topology

The topology display visualizes the arrangement and connection statuses of monitored devices based on information that SINEMA Server calls up from the devices via SNMP and PROFINET. The PROFINET device names of the devices may be required to generate the topology display and must therefore be unique. This also applies when the PROFINET monitoring is disabled in SINEMA Server.

Topology modes

Based on data obtained by SINEMA Server in the Editing mode a reference topology can be configured in which the devices involved and target statuses for connections and ports can be set. Devices and connections that were defined as part of the reference topology are known below as reference devices and reference connections. Reference connections and statuses for ports can only be configured for reference devices.

In Online mode you can monitor the network taking into account the configured reference topology. For connections and ports of reference devices deviations between detected statuses and reference statuses are highlighted by SINEMA Server and communicated using corresponding events. These events can influence the overall status of the reference devices, see section Administration - Events Overall status groups (Page 200).

Display of devices and connections.

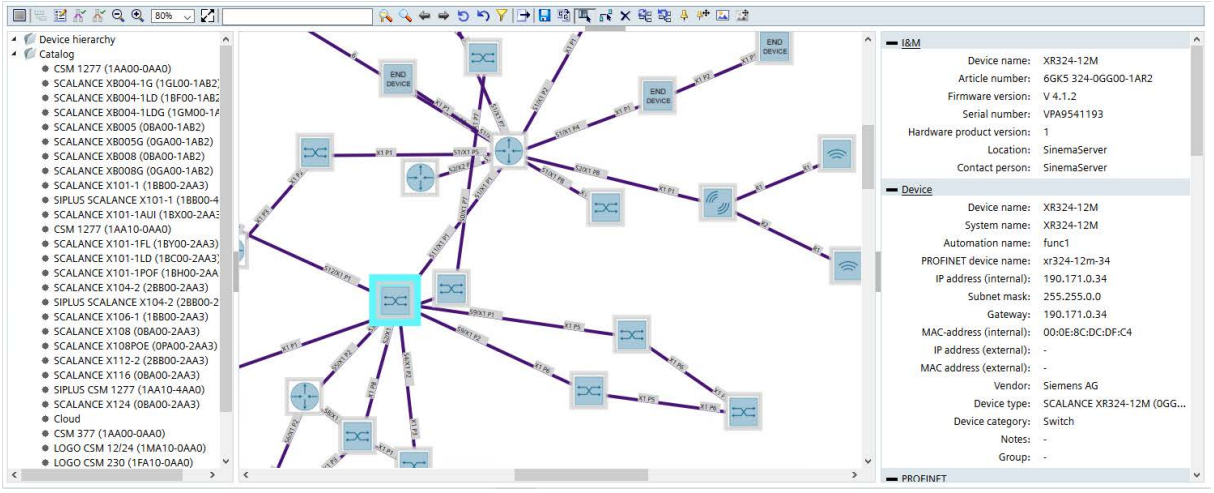
In both topology modes, SINEMA Server places detected devices in the topology display and networks them together based on their detected connections. SINEMA Server uses a form of display based on the equilibrium of forces between nodes and connections. The resulting device distribution can be changed in Editing mode. Each device is represented by a node with an associated device icon. In both topology modes devices that are not part of the reference topology are displayed with a star symbol, reference devices are displayed without a star symbol.

Devices without detectable connection information are displayed by SINEMA Server separated from the networked devices in the topology display. If a device without a detectable IP address is connected to three or more devices, the device without a detectable IP address is represented by a cloud symbol.

If devices are shown as overlapping in the topology, you can adjust the topology size in editing mode, see section Operator input (Page 136).

Available work areas

The following figure illustrates the division of the work areas based on the Editing mode.



In the Editing mode, the device hierarchy in the left side bar is initially empty, all detected devices are located in the topology display. If these devices are deleted from the topology display using the shortcut menu, they appear in the device hierarchy and can be dragged to the topology display again. In the Online mode the device hierarchy displays all devices with their IP addresses, device names and overall statuses that are located in the topology display.

In the Editing mode, the left side bar contains a device catalog for adding unmanaged devices. Unmanaged devices that were added in "Topology > Unmanaged devices" are available in this catalog. This involves devices that cannot be monitored by SINEMA Server and that can be inserted to complete the topology display. Added unmanaged devices are displayed in the topology display of both topology modes.

After selection of a device in the topology display, the right-hand side bar shows the details of the device, ports as well as events pending for the device. In the Editing mode, the reference statuses for device ports can be configured in this detail area, refer to the section Editing mode (Page 136).
By double-clicking on a device in the topology display the device details of this device are called up.

The following sections describe the Editing and Online modes in detail.

4.2.1 Editing mode

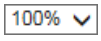
4.2.1.1 Operator input

If no reference topology has yet been created, and you have the right "operative monitoring settings", the topology is displayed after selecting the "Topology" menu command in the Editing mode. The following sections explain how to work with the toolbar and port overview in this topology mode.

Toolbar

Operator control element	Function
	Editing mode When you click on the operator control element, SINEMA Server switches to the Online mode. If there are unsaved changes to the reference topology, you can save these in a dialog before the switchover.
	Extended icon view As default the icon view is enabled in which the icon for the device type and the overall status of the device is displayed. In the extended icon view, in addition to this up to three device properties configurable in the topology settings are displayed.

Operator control element	Function
	Topology settings • Display connections: Show/hide all connections When the check box for the connection display is disabled, the check box for displaying the port names is automatically disabled and cannot be enabled. • Display port names: In the topology display the names of the ports between which connections exist are displayed. With this option, you can show / hide these names. • Show next update in online mode: Show / hide circular icon for the progress of the automatic update of the topology display in the Online mode. The circular icon shows when the interval for the automatic update has elapsed. This can be configured in "Administration > My settings > User interface". In the Editing mode, the topology display is not updated automatically. This happens when saving and when updating manually using the menu bar. • Show synchronization connection between SIMATIC S7-400-H CPUs: An orange dashed line is shown between redundantly configured SIMATIC S7-400-H CPUs of an H system when this check box is selected. This line represents the two POF cables used for synchronization between the CPUs. In case of a synchronization error, the line is shown with a red border. To display the synchronization connection, SIMATIC monitoring must be activated for both CPUs of the H system. • Device icon style in topology: Specifies the style for the icons with which devices are shown in the topology display: – Device category: The devices are displayed with the icons of their associated device categories. Device categories can be set in the device profile editor. The assignment of icons to device categories cannot be adapted. – Device profile: The devices are displayed with icons that are assigned to the associated device types in their device profiles. If no matching icon exists for a device type, the default profile icon of the device profile is used. • Device labeling: Selection of up to three device properties that are displayed in the extended icon view for devices. • Size of the topology grid: Specifies the size of the cells of the topology grid in the Editing mode. Devices can only be moved along these grid cells. This setting does not change the existing position of devices. • Move surrounding devices When moving selected devices in the Editing mode, surrounding devices that are not fixed can also be moved automatically to maintain the device distribution. With this option you specify whether or not these surrounding devices are moved. – Do not move (Default setting): When moving selected devices, the surrounding devices are not moved. This option is recommended with large networks / topologies since there is no recalculation of the position and therefore the topology display is available more quickly. – During moving: When moving selected devices, the surrounding devices are moved to the suitable positions. – After moving After moving selected devices, the surrounding devices are moved to the suitable positions. Due to the recalculation of the position, the topology display is available after a delay.

Operator control element	Function
	• Topology size: Specifies the clearances and the length of the connections between the devices in the Editing mode. A higher setting means greater clearances and longer device connections. The topology size should be selected according to existing number of devices. After changing the topology size, the device positions are recalculated. – Dynamic: SINEMA Server selects the topology size itself according to the existing number of devices. – Small: Up to 100 devices – Medium: 100 to 250 devices – Large: More than 250 devices – User-defined: You specify the topology size with a slider. By moving the slider to the right, you create greater distances between the devices, longer device connections and therefore fewer overlaps between the devices.
	Current connections are displayed Detected, active connections between devices are displayed. If the check box "Display connections" is disabled in the topology settings, this option cannot be enabled.
	Learned connections are displayed Learned connections between alternating devices and tool changer devices are displayed. If the check box "Display connections" is disabled in the topology settings, this option cannot be enabled.
	Reduce topology view With each click the topology view is reduced by one zoom level.
	Enlarge topology view With each click the topology view is enlarged by one zoom level.
	Select zoom level
	Match zoom level to topology Select a zoom level that shows the entire topology without scrolling.
	Device scan Searches for the entered text in the device properties of the devices in the topology display. To speed up the search, you can limit the search with the icon to the device properties for which you want to search. You start the search with the icon. Matching devices are displayed in a hit list and highlighted in the topology display. The device whose details are displayed in the right-hand side bar is highlighted in the topology display as well as in the hit list. To search for devices in IP address ranges, the following format must be kept to: IP address1 - IP address2 The spaces after and before the IP addresses are optional.
	Previous device / Next device If several devices were found in the device scan, the previous / next device can be selected with these operator input elements. The device details of this device are then shown in the right-hand side bar. Alternatively, the required device can be selected in the hit list of the device search.
	Reset device scan and scan results Deletes the input text of the device scan and deselects selected devices in the topology display.

Operator control element	Function
	Undo last action Undo the last action in the topology.
	Topology filter Opens a dialog in which you can manage device groups. Monitored devices can be assigned to a device group. After selection of a device group in online mode, the associated devices are highlighted with a dark blue border. You can also manage device groups and assign devices to device groups with the device shortcut menu item "Assignment to device groups".
	Export topology Exports the topology display as a *.PNG file ina *.ZIP archive. The set zoom level is always used. The topology display is always exported with a transparent background. The background color of the exported topology display depends on the display software used.
	Save Saves the configured reference topology and updates the topology display.
	Adopt detected statuses as reference statuses Adopts all the statuses detected by SINEMA Server in the reference topology: • Detected devices are adopted as reference devices. The star symbols are removed from the devices. Individual devices can be adopted as reference devices using the shortcut menu. • Detected port statuses are adopted as reference statuses. The reference statuses of ports can be set manually in the port overview of the right-hand side bar, see section "Configuring reference statuses for ports". • Current / learned connections are adopted as reference connections. Partial connections are not adopted as reference connections. Individual reference connections can be adopted as reference connections with the shortcut menu or by double-clicking. The connected devices automatically become reference devices. If the connection to be adopted is a partial connection, the connection wizard is called in which you can specify the ports of the reference connection.
	Selection tool As default the selection tool is enabled. With the selection tool you can move devices along the configured topology grid by dragging them. As default after they have been moved devices are fixed in the topology display. When moving devices the device clearance is maintained, that is preset by the topology size configured in the topology settings. Using the shortcut menu of reference connections between fixed devices bending points can be inserted with which the course of the connections can be adapted. To do this drag the bending points to the required position. If a bending point is inserted on a reference connection between devices that are not fixed, the devices are fixed automatically. A maximum of 10 bending points per connection and 1000 bending points per topology can be created. With the shortcut menu command "Reset connection layout" the course of the connection is reset to the initial status. Individual bending points can also be deleted using the shortcut menu. If the fixing of a device is canceled, the bending points of the corresponding reference connection are deleted. Using a very large number of bending points slows down the topology display.

Operator control element	Function
	Drawing tool With the drawing tool you can draw reference connections between reference devices manually. To do this, click on the devices to be connected one after the other to call the connection wizard to select the ports involved. By selecting them with the drawing tool devices automatically become reference devices. In the connection wizard the ports of the devices to be connected are displayed with their detected and configured port statuses. Which of the ports are already connected is not displayed in the connection wizard but by the port names in the topology display. In the connection wizard click on the ports that are to be connected one after the other Per device one port can be selected, selected ports are highlighted in blue. If you draw a connection from an already connected port to another port of the same partner device, the connection is changed. Several connections of a port to different ports of the same device cannot be drawn. If you draw a connection from an already connected port to the port of a device to which there is not yet a connection, you can decide whether the existing connection is changed or whether an additional connection should be added. If the connection should be added, the port with more than one connection is automatically configured as a docking port. For ports already configured as docking ports in the case described the additional connection is generated as standard. Devices connected to docking ports are automatically configured as alternating devices. It is possible to draw link aggregations between devices. To do this the connection wizard must be used once per connection to be added. It is only possible to delete reference connections via the shortcut menu of the connections.
	Delete learned connections Deletes all learned devices from the reference topology. After deleting, the learned connections are also no longer visible in the Online mode. Individual learned connections can be deleted using the shortcut menu. If the check box "Learn connections of alternating devices automatically" is enabled in "Administration > Monitoring > General" the connections are learned again.
	Recalculate device positions Arranges all non fixed devices in the topology display with the aid of the distribution algorithm. This makes sense after adding devices step by step or after deleting devices from the topology display.
	Reset reference topology Resets the configuration of the reference topology: • All devices are removed from the reference topology and displayed with a star symbol. Individual reference devices can be removed from the reference topology using the shortcut menu. • All configured reference statuses for ports are reset • All reference connections are removed. Individual reference connections can be removed using the shortcut menu.

Operator control element	Function
	Fix selected devices As default, detected devices are not fixed. Non fixed devices are possibly repositioned automatically by moving other devices, by recalculating device positions and possibly by adding and removing devices. Fixed devices are not repositioned in these situations. Fixed devices are shown with a pin symbol. If this tool is used on devices that are already fixed, the fixing of these devices is canceled. Bending points on reference connections belonging to these devices are deleted. If there are both fixed and non fixed devices among the selected devices, using this tool fixes all devices. As an alternative the fixing can be set using the shortcut menu.
	Fixing devices after moving them. As default this tool is enabled. After moving them, devices are fixed.
	Insert background picture Inserts a background picture in the top left corner of the topology display. Maximum size: 50 MB Maximum resolution: 5000 x 5000 pixels An already inserted background image can be deleted, updated and, after activating the tool  , moved and resized via the shortcut menu.
	Move background image / change size of background image After changes have been made, the topology display must be saved.

Configuring reference statuses for ports

Reference statuses can only be configured for ports of reference devices. Using the shortcut menu of the ports, the following reference statuses can be configured in the "Port overview" area of the right-hand side bar:

- Up
- Down (cannot be selected if a reference connection exists)
- Unmonitored (only for LAN ports):
  - Port connection statuses are not monitored
  - Events relating to port reference statuses are not displayed
- Docking port (only for LAN ports):
  - Port connection statuses are not monitored
  - Events relating to port reference statuses are not displayed
  - Connections of this port are learned when in "Administration > Monitoring > General" the check box "Learn connections of alternating devices automatically" is enabled.

See also

Colors and icons (Page 142)

4.2.1.2 Colors and icons

Ports

In the "Port overview" area of the right-hand side bar, the detected statuses and the configured reference statuses of the ports of the selected device are displayed. The detected statuses are symbolized by the frame color, the reference statuses by the fill color of the ports. The table below shows the meaning of the possible port colors of reference devices.

Detected status	Configured reference status		
	Up	Down	Docking port / unmonitored port
Active			
Inactive			
Unknown			
Docking port / unmonitored port			

If the corresponding devices are not part of the reference topology, the fill color of the ports is white.

Connections

Current connections are shown in violet, learned connections in brown and reference connections in black. If several connection types apply, the relevant connection colors are shown as a combination. If the current and the learned connection type apply only the current connection is displayed.

So that current connections and learned connections are shown, the corresponding options in the toolbar must be selected. To display learned connections, in "Administration > Monitoring > General" the check box "Learn connections of alternating devices automatically" must also be enabled.

Synchronization connections

An orange dashed line is shown between redundantly configured SIMATIC S7-400-H CPUs of an H system. This line represents the two POF cables used for synchronization between the CPUs. In case of a synchronization error, the line is shown with a red border. To display the synchronization connection, SIMATIC monitoring must be activated for both CPUs of the H system. In addition, the topology setting "Show synchronization connection between SIMATIC S7-400-H CPUs" must be enabled.

4.2.2 Online mode

4.2.2.1 Operator input

If a reference topology is already available, the topology is displayed in Online mode after selecting the "Topology" menu command. The majority of the operator input elements available in Online mode also exist in the Editing mode, see section Editing mode (Page 136). The operator input elements and shortcut menu commands for configuration of the reference topology are only available in the Editing mode. The following operator input elements are only available in the Online mode:

Operator control element	Function
	Online mode When you click on the operator control element, SINEMA Server switches to the Editing mode.
Update interval (in topology settings)	In online mode, you can specify the interval at which the user interface of the topology is going to be updated. The following options are available: • Dynamic: For 250 devices or less, the update interval is 15 seconds. As of 251 devices, the update interval is 30 seconds. • 15 seconds • 30 seconds • 45 seconds • 60 seconds The circular icon in the status bar shows when the interval for the automatic update has elapsed.
	Topology filter Filter for highlighting devices and connections. The following filter categories are available: • VLAN: After selecting a VLAN ID, all associated devices and connections are highlighted in dark blue. You can only filter for one VLAN ID at a time. • Device groups: After selecting a device group, all devices that were assigned to the device group in editing mode are highlighted in dark blue and displayed in the right-hand side bar. The device groups to which a device is assigned can be seen with the shortcut menu command "Member in device groups" of this device as well as in the right-hand side bar.

4.2.2.2 Colors and icons

Devices

In the Online mode, the entire statuses of the devices are displayed with frame colors. This applies regardless of whether or not the devices were added to the reference topology. The meaning of the icons fro the overall device status are described in section Device tree (Page 92).

Ports

In the "Port overview" area of the right-hand side bar for devices that were not added to the reference topology, only the detected statuses of the ports are displayed. The detected statuses decide the frame and fill colors of the ports. The same colors are used as for the detected statuses in the Editing mode, see section Colors and icons (Page 142).

For reference devices the detected statuses and the statuses resulting from the detected statuses and the configured reference statuses are displayed. The detected statuses are symbolized by the frame color, the resulting statuses by the fill color of the ports. The table below shows the meaning of the possible port colors of reference devices:

Detected port status	Reference port status	Resulting port status		Border color / fill color
Active	Active	Active		
Active	Inactive	Active - Maintenance required		
Active	Docking port / unmonitored port	Docking port / unmonitored port		
Inactive	Active	Inactive - Maintenance required	With current connection	
			Without current connection	
Inactive	Docking port / unmonitored port	Docking port / unmonitored port	With current connection	
			Without current connection	
Inactive	Inactive	Inactive	With current connection	
			Without current connection	
Unknown	-	-		
Docking port / unmonitored port	All reference port statuses	Docking port / unmonitored port		

The table below shows the meaning of the colors of redundant ports for devices that were not added to the reference topology:

Current connection exists	Detected port status	Redundancy status	Port color
Yes	Active	Disabled	
		Blocking / discarding	
		Forwarding, listening, learning, unknown	
		Not connected / broken	
		Warning	
Yes	Not active (can be a temporary status until the connection was calculated)	Disabled / broken / discarding	
		Blocking	
		Forwarding, listening, learning, unknown	
		Not connected	
		Warning	
No	Active (can be a temporary status until the connection was calculated)	Disabled	
		Blocking / discarding	
		Forwarding, listening, learning, unknown	
		Not connected / broken	
		Warning	
No	Inactive	Disabled / broken / discarding	
		Blocking	
		Forwarding, listening, learning, unknown	
		Not connected	
		Warning	

The table below shows the meaning of the colors of redundant ports for devices that were added to the reference topology:

Resulting port status	Redundancy status	Border color / fill color
Active	Disabled	
	Blocking / discarding	
	Forwarding, listening, learning, unknown	
	Not connected / broken	
	Warning	
Active - Maintenance required	Disabled	
	Blocking / discarding	
	Forwarding, listening, learning, unknown	
	Not connected	
	Warning	
Inactive	Disabled / broken / discarding	
	Blocking	
	Forwarding, listening, learning, unknown	
	Not connected	
	Warning	
Inactive - Maintenance required	Disabled	
	Blocking / discarded	
	Forwarding, listening, learning, unknown	
	Not connected	
	Warning	

Connections

Connection colors

The connection lines in the Online mode correspond in terms of the connected ports to the connection lines in the Editing mode. If a reference connection between two ports does not

correspond to the current connection or one of the learned connections, the connection color is red regardless of the fill colors of the ports. Otherwise the connection color is based on the fill color of the two connected ports. Which of the port colors decides the color of the connection line depends on the priority of the port color:

- Red (highest priority)
- Yellow
- Blue
- Green
- Gray
- White (lowest priority)

With unmonitored ports / docking ports, the connection color is defined by the status of the partner port.

Learned connections that are not active at the time of the display between tool changer devices and alternating devices are displayed as follows regardless of the color of the connected port.

- Learned connection was not adopted as reference connection: Brown
- Learned connection was adopted as reference connection: Gray

Learned active connections are displayed in green.

Table 4- 22 Connection colors of WLAN connections

Reference connection active	Connection color
No	Light gray
Yes	The color of an active reference connection is based on the port color (green, red or light gray). Light gray: The user has specified in the reference that a connection can exist. Green: Connection discovered as active by SINEMA Server. Red: One of the interfaces belonging to the connection is down.

A reference connection is treated as an active connection if one of the reference connections corresponds to the actual WLAN connection. The color of the active connection is based on the color of both ports. Yellow and dark gray are used to indicate an invalid port status if a reference connection is defined. All other reference connections between a client and several APs that are down are shown in gray. Which of the port colors decides the color of the active connection between client and AP depends on the priority of the port color:

- Red (highest priority)
- Green
- Gray (lowest priority)

Connection types

Electrical connections, optical connections, wireless connections and unknown connections are shown in the Online mode view as follows:

Connection type	Description
	Wireless connection
	Optical connection
	Electrical connection
	Unknown connection
	Synchronization connection between SIMATIC S7-400-H CPUs, see the section "Synchronization connections" below.

The types of the connected ports decide the type of connection displayed. Which of the port types decides the type of connection depends on the priority of the port type:

- Electrical (highest priority)
- Optical
- Wireless
- Unknown (lowest priority)

Synchronization connections

An orange dashed line is shown between redundantly configured SIMATIC S7-400-H CPUs of an H system. This line represents the two POF cables used for synchronization between the CPUs. In case of a synchronization error, the line is shown with a red border. To display the synchronization connection, SIMATIC monitoring must be activated for both CPUs of the H system. In addition, the topology setting "Show synchronization connection between SIMATIC S7-400-H CPUs" must be enabled.

4.2.3 Special features

Partial connections

A partial connection is a connection in which the connection port of at least one device is unknown. The following types of partial connections must be distinguished:

- Type A: Port-to-device connection
- Type B: Device-to-device connection

Partial connections are displayed according to the same rules as conventional connections. Partial connections cannot be adopted immediately as reference connections. First the ports involved must be selected in the connection wizard.

In Online mode, the color of an expanded reference connection is formed by comparing it with the discovered connection information. For partial connections of type A, the connection color is decided by the fill color of the port if the connection information matches up:

Connection type	Match with the discovered connection	Fill color of the port	Connection color
A	Yes	Green	Green
A	Yes	Not green	Fill color of the port
A	No	Every fill color	Red
B	Yes	-	Gray
B	No	-	Red

High availability (HA) PROFINET IO devices

The PROFINET interface modules of an HA device are shown in the topology as device pair if the interface modules were not fixed manually to different positions. To detect HA devices, PROFINET monitoring must be enabled for them, see section Administration - Monitoring General (Page 186).

4.2.4 Unmanaged devices

In "Topology > Unmanaged devices", you can manage devices that cannot be monitored by SINEMA Server and that can be inserted in the topology display to complete the representation. In Editing mode of the topology page, the devices in "Topology > Unmanaged devices" are available in the left side bar. Inserted unmanaged devices are also displayed in Online mode.

4.3 Reports

Types of report

SINEMA Server provides a set of reports for network monitoring and analysis. Specifically, the following properties and criteria are analyzed:

- Availability
- Performance
- Inventory
- Events
- Validation reports

In the report types “Availability”, “Performance”, “Inventory” and “Events” you can select the data to be evaluated more precisely based on the form, content and time period. The reports can be used to display statistical data in tables or graphic diagrams. Depending on the selected report type analog and digital graphs (pulse line) are displayed. You can create a

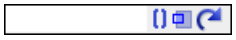
preview of a report and print it out. The pages with the generated reports contain information in various boxes displayed in the table view. Optionally, this information is also shown as a pie chart or bar chart. Depending on the filter criteria the appropriate boxes are displayed with report information. The following information in the section, relates to the Web pages of the four report types mentioned.

For information on validation reports, refer to the section Reports - validation reports (Page 159)

Operation / content

The following table shows the functional elements of the header in the tabs for reports.

The reports contain a selection of the following function elements:

Icon	Display / function	Icon	Display / function
	Show/hide graphic		Show/hide table
24 hour	Evaluation time period: 24 hours	7 day	Evaluation time period: 7 days
	Enter text to filter based on data records. The entered text is searched for in all columns. In the input box, text is displayed when a simple query entered in the filter template editor is active. The icon is displayed when a filter template with prefilter settings is active. The {} icon is displayed when a filter template with a complex query is active.		Selection of a previously created template for filtering according to data records. After selection, the properties of the filter template are applied to the report. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
	Open the editor for configuring filter settings that can be stored in filter templates. The icon is displayed when the configured filter settings differ from the default filter settings. You will find further information in the sections on the individual report types.		

Note

Validity of the filter settings

The filter settings made on these pages remain valid until you log out from the application. If you change the filter settings, these also remain valid if you change back and forth between Web pages.

Printing reports

When you select the report function, the function element for the print function appears in the status bar.

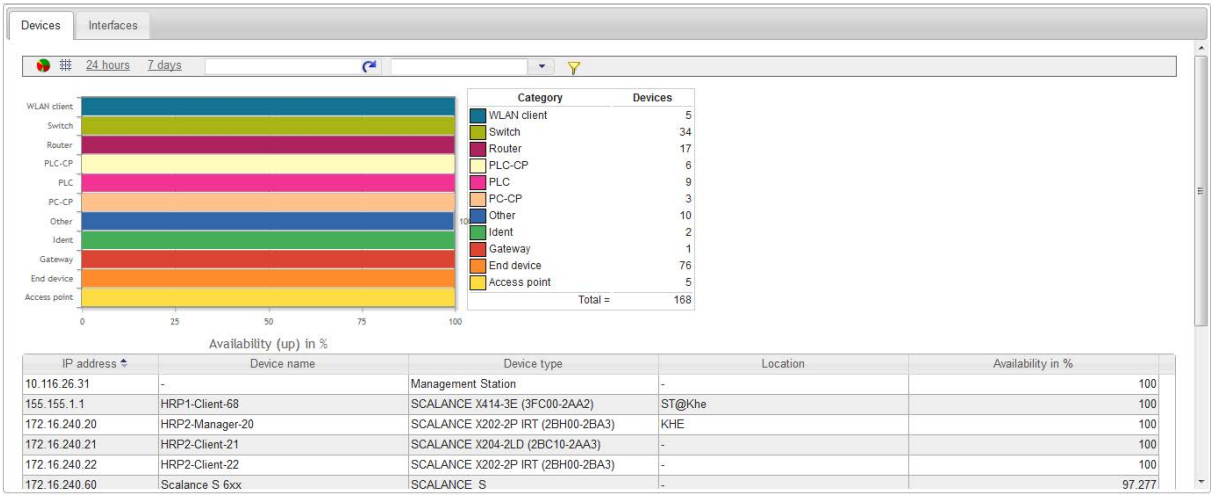
SINEMA Server outputs the content of the currently displayed report Web page in a new Web page. There, you can select further output methods with the functions available in your Web browser, for example, output to printer or to a PDF file.

Archive management

Historical data for creating reports is stored in the system database. In the management station, the SINEMA Server Monitor provides a function with which you can delete, swap out or import historical data.

4.3.1 Reports - Availability

The report types described below are available with the menu command: **"Reports > Availability"**



Meaning

Display of all (filtered) objects with information relating to their availability; in other words, how long they were reachable during the monitoring period. In addition to the table display, a graphic is also generated in which the monitored objects are evaluated again in groups.

"Devices" tab

The display is limited to complete devices regardless of their individual ports. The grouping in the graphic is according to device groups (routers, switches, access points etc.).

"Interfaces" tab

In this tab, the operating time of monitored interfaces is shown as a percentage. The interfaces are shown grouped according to the transmission media. When calculating the percentages for the operating time the interfaces potentially available for a device are used as the maximum value.

If a user-defined name was assigned for an interface, this is shown in the default "Name" column instead of the discovered name.

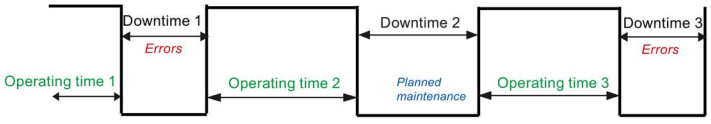
Operation / content

Although the column assignment in the data area is preset, you can arrange it any way you require (in the footer). Except for the "constant" information as it appears in the Device details, for example, you can also select the following statistical values:

- Availability (percentage)
- Number of outages
- Total uptime (period absolute)
- Total inactive (period absolute)
- Last discovered
- First discovered
- Average downtime (period absolute)
- Average uptime (period absolute)
- Unmonitored period (period absolute)
- Not monitored (percentage)
- Device deleted (information, whether and when deleted)

Calculations for the availability report

The availability report provides report data relating to the availability of devices in the network. To be able to calculate this information about device availability, the total operating time or the total downtime of a device must be known. The calculation of the availability report is based on the average operating time and the average downtime of devices and interfaces.



Average operating time = total operating time / total downtimes

Total operating time = operating time 1 + operating time 2 + operating time 3 + …

Average downtime = total downtime / total failures

Total downtime = downtime 1 + downtime 2 + downtime 3 + …

The downtime can be caused by failures or planned downtimes.

% availability = average operating time * 100 / (average operating time + average downtime)

Prefilter for reports on availability

Reports on availability can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for availability reports. You will find basic information on filter templates and the options of using complex filters in the section "Filtering data with filter templates" of the operating instructions of SINEMA Server.

Table 4- 23 Filters for availability reports in the "Devices" tab

Operator control element	Filter options
Device	Filtering according to existing or deleted devices.
Period	Filter according to data records of the last 7 days / 24 hours / period entered manually.

Table 4- 24 Filters for availability reports in the "Interfaces" tab

Operator control element	Filter options
From IP To IP	Filter according to data records that have the specified IP addresses.
Device name, device type and device category	Filter according to data records for interfaces that belong to devices with the specified device name, the device type or the device category.
Statistics activated	Filter according data records for interfaces for which the port statistics are activated /deactivated: • All • Yes: Interfaces with activated port statistics • No: Interfaces with deactivated port statistics
Device	Filtering according interfaces belonging to existing or deleted devices.
Port status	Filter according to interfaces with an active connection status: • All • Only interfaces with an active connection status
Period	Filter according to data records of the last 7 days / 24 hours / period entered manually.

See also

Filtering data with filter templates (Page 77)

4.3.2 Reports - Performance

The report types described below are available with the menu command: **"Reports > Performance"**

Structure and meaning

Display of the performance of monitored interfaces; in other words, how fast and reliably they have transferred and received data during the monitoring period. To display the reports the statistics for the interfaces must have been enabled in the "LAN" tab of the device details.

- LAN - Interface utilization:
  For all LAN interfaces, not only the maximum possible speed but also their total load when sending and receiving is displayed.
- LAN - Interface quality:
  The error quota when sending and receiving is displayed for all LAN interfaces.
- WLAN - Interface quality:
  The error quota when sending and receiving is displayed for all WLAN interfaces.
- WLAN - Interface data rate (transmission speed):
  For all WLAN interfaces, the bandwidth (data rate) when sending and receiving is displayed.
- WLAN - Number of clients:
  For all access points, the number of WLAN clients to which they were connected on average is displayed.
- Discarded packets:

  The number of discarded incoming packets and the number of discarded outgoing packets is displayed for all LAN and WLAN interfaces.
- POF power budget:

  For LAN interfaces of the type "Plastic Optical Fiber (POF)", information about the power budget is displayed.

Operation / content

Although the column assignment in the data area is preset, you can arrange it any way you require (in the footer). Except for the "constant" information as it appears in the Device details, for example, you can also select the following statistical values:

- Average transmission performance (%)
- Average reception performance (%)
- Average performance (%)
- Maximum transmission performance (%)
- Maximum reception performance (%)
- Maximum performance (%)
- Average error rate (%)
- Maximum error rate (%)
- Average transmission error rate (%)
- Average reception error rate (%)
- Maximum transmission error rate (%)
- Average POF power budget
- Maximum reception error rate (%)
- Average transmit data rate (Mbps)
- Current transmission data rate (Mbps)
- Maximum transmission data rate (Mbps)
- Average signal strength (dBm)
- Maximum signal strength (dBm)
- Average client number
- Maximum client number
- Mode (WLAN default)
- Used channel
- Information if and when deleted
- Maximum POF power budget

Special feature

If the "Historical data" box is also displayed, you can use the shortcut menu of this icon to generate a further diagram in which the data that has already been recorded can be further analyzed.

Prefilter for reports on performance

Reports on performance can be filtered with the aid of filter templates. You will find basic information on filter templates and the options of using complex filters in the section "Filtering data with filter templates" of the operating instructions of SINEMA Server.

The meaning of the settings of the prefilter for reports on performance can be found in the section on the "Availability" report type.

See also

Reports - Availability (Page 151)

Filtering data with filter templates (Page 77)

4.3.3 Reports - Inventory

The report types described below are available with the menu command: **"Reports > Inventory"**

Layout

The **"Reports > Inventory"** Web page contains the "Vendor", "IP address range", "Device category" and "PROFINET" tabs.

meaning / content

Inventory reports contain information relating to the vendor, IP range and device category for all the devices discovered in the network during the selected period.

Although the column assignment in the data area is preset, you can arrange it any way you require (in the footer). The following can be selected:

- IP address
- Device name
- Device type
- Location
- Name of the IP address range
- Number of interfaces (used / total)
- PROFINET device name
- MAC address
- Firmware version
- Article number
- Historical data

In the "PROFINET" tab, the following additional columns can be selected:

- PNIO name
- Device category
- PNIO role
- Subnet mask
- Router address
- Assigned PLC

Prefilter for reports on the inventory

Reports on the inventory can be filtered with the aid of filter templates. You will find basic information on filter templates and the options of using complex filters in the section "Filtering data with filter templates" of the operating instructions of SINEMA Server.

In the prefilter of reports on the inventory, you can filter according to monitored or unmonitored devices.

See also

Filtering data with filter templates (Page 77)

Reports - Availability (Page 151)

4.3.4 Reports - Events

The report types described below are available with the menu command: **"Reports > Events"**

Layout

The **"Reports > Events"** Web page contains the "Network events" and "System events" tabs.

Meaning

Display of all the events that have occurred (filtered) with information relating to the status, event type and the time it occurred. In addition to the table, a graphic is also generated in which the monitored events are regrouped (error, warning etc.).

Predefined report forms (tabs):

- Network events:

  All network events are displayed; in other words, messages generated by the network devices.

- System events:

  All system events are displayed; in other words, the messages generated by SINEMA Server.

Prefilter for reports on events

Reports on events can be filtered with the aid of filter templates. This section deals specifically with the available settings of the prefilter for availability reports. You will find basic information on filter templates and the options of using complex filters in the section "Filtering data with filter templates" of the operating instructions of SINEMA Server.

Table 4- 25 Filtering reports on events

Operator control element	Filter options
Basic filter settings	Read: • Yes • No • All Event state: • All • " - " • Resolved automatically • Resolved manually • Pending Period: Filter according to events • Unlimited • the last X hours • the last X days • immediately • of a manually entered time range X: Number specified by the user From device: Filter according to deleted or existing devices
Event classes	Filter according to the severity of events: • Notification • Information • Warning • Error

Operator control element	Filter options
Protocols	Filter according to protocols by which the events were triggered: • ICMP • DCP • ARP • SNMP • SNMP trap • PROFINET • SIMATIC • Multiple (event was triggered by more than one protocol) • SIMATIC event messages • SIMATIC alarm messages

See also

Filtering data with filter templates (Page 77)

4.3.5 Reports - validation reports

4.3.5.1 Overview

Function of validation reports

A validation report is the result of a configurable collection of validation is with which monitoring data of different categories can be checked based on configurable criteria. The priority can be defined for every selected validation. With the priority, you specify whether or not the result of a validation is relevant to the overall result of the validation report.

Parts of validation reports

A validation report is created in the form of a PDF file and validation report attachments and can be downloaded in the ZIP format from SINEMA Server

The PDF file contains the overall result of the validation report, a validation overview and if applicable the results of validations that were not passed. The overall result indicates whether the validation is of the validation report were passed in total. This is the case when all validations with the validation priority "Obligatory" were passed. The validation overview indicates which validations were performed, whether these were passed, for how many devices, ports or events the relevant validation was performed and how many did not meet the criteria of this validation. In the results of validations that were not passed the data is highlighted in red due to which the relevant validation did not pass.

The validation report attachments contain all data in the .XLSX format that were used to obtain the results of the validations performed.

4.3.5.2 Validation report configurations

Layout of the Web page

After selecting the "Reports > Validation reports" web page, the "Validation report configurations" tab displays the configurations of validation reports with their status information, properties, and file sizes. If the logged-on user does not have the right to "View all devices and servers", only the validation report configurations to which a user view is assigned are displayed.

With the control elements of the header, validation report configurations can be managed and the corresponding validation reports downloaded,

Operator input

The following table explains the control elements of the header of the tab.

Control element	Function
	Adding a new validation report configuration The dialog for validation report configurations is opened, refer to the section Configuration of validation reports, and validation report templates (Page 162). With the configurations of validation reports, and validation report templates, the same validations an be selected and configured.
	Copying a selected validation report configuration The selected validation report configuration is copied and the configuration dialog for the new object is opened. The settings of the copied object are adopted and can be adapted.
	Editing a selected validation report configuration The dialog for validation report configurations is opened, refer to the section Configuration of validation reports, and validation report templates (Page 162).
	Deleting a selected validation report configuration The selected validation report configurations are deleted. By deleting validation report configurations. the corresponding validation reports are also deleted. Validation reports in the “In progress” status cannot be deleted.
	Displaying a selected validation report configuration The dialog for configuration of the validation report opens. No changes can be made.
	Displaying the PDF file The PDF file for the validation report created for the selected validation report configuration is displayed in a new tab of the Web browser. Displaying PDF files is only possible for validation reports in the status "Finished". A suitable PDF reader is required to display PDF files.
	Downloading validation report The validation report for the selected validation report configuration is downloaded including the validation report attachments in ZIP format. Multiple selection is possible. Downloading validation reports files is only possible for validation reports in the status "Finished". The text box "Size of the selected validation reports (MB)” shows the file size of the validation reports of all validation report configurations.
	Searches the list of validation report configurations for the entered text.

4.3.5.3 Validation report templates

Layout of the Web page

To simplify the creation of validation report configurations, in the "Validation report templates" tab, you can create templates that can be used and adapted when creating validation report configurations. If the logged-on user does not have the right to "View all devices and servers", only the validation report templates to which a user view is assigned are displayed.

Operator input

The following table explains the control elements of the header of the tab.

Control element	Function
	Adding a validation report template The dialog for validation report templates is opened, refer to the section Configuration of validation reports, and validation report templates (Page 162). With the configurations of validation reports, and validation report templates, the same validations an be selected and configured.
	Copying a selected validation template configuration The selected validation report template is copied and the configuration dialog for the new object is opened. The settings of the copied object are adopted and can be adapted.
	Editing a selected validation template configuration The dialog for validation report templates is opened, refer to the section Configuration of validation reports, and validation report templates (Page 162).
	Deleting selected validation template templates The selected validation report templates are deleted.
	Searches the list of validation report templates for the entered text.

4.3.5.4 Configuration of validation reports, and validation report templates

Overview

You can use the buttons for creating, editing or copying validation report configurations and templates to reach the dialog in which the validations to be made can be configured. The available validations are assigned to categories whose content you can hide and display using the PLUS and Minus sysmbols. The categories and the validations they contain are displayed in an overview tree in the left area of of the configuration dialog. By selecting an entry in this tree, you come directly to the relevant position of the configuration dialog. Before a validation can be configured, the corresponding check box must be enabled. After enabling a validation, its priority can be specified by clicking the symbol in front of the check box. The symbols have the following meaning:

Symbol	Meaning
	Validation priority “Obligatory” A validation with this priority relevant for the overall result. The validation must have passed, so that the overall result “Passed” can be reached.
	Validation priority “Optional” A validation with this priority is not relevant for the overall result. Validation reports that only contain validations with this validation priority always have the overall result “Passed”.

Configuration settings

For validation report configurations, you can select a validation report template in the “Configuration settings” area. So that the template settings are adopted, you need to click the “Use validation report template” button after selecting a validation report template.

When you select a view from the "View" drop-down list for validation report configurations and validation report templates, only the data from the devices in this view are included in the validation. If the logged-on user does not have the right to "View all devices and servers", only the views assigned to this user are available for selection in the drop-down list.

Before saving a validation report template you need to specify its name in the “Configuration settings” area.

Basic settings

In the basic settings of the configuration dialog, you can enter information about the company and the plant to which the data to be evaluated by the validation report is assigned. You can also specify the degree of trustworthiness of the validation report. The specified information appears in the PDF file generated for the validation report. For validation report configurations, the name of the validation report to be generated must be specified in the basic settings. The PDF file generated for the validation report configuration is given this name.

Generate picture of topology

In this area you can specify whether SINEMA Server should generate a picture in the PNG format from the topology display and include this in the validation report attachment. The picture is generated in the Online mode. You can choose whether the picture is generated from the icon view of the extended icon view.

The following sections explain the configurable validations. The table column “Description of the validation” always names the scenario in which a validation fails.

After configuring a validation report, its creation can be started with the “Generate validation report” button. As an alternative, the settings made can be saved as a validation report configuration or as a validation report template.

Device properties

The following validations can be configured in the “Device properties” category:

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
White list for firmware versions	For all monitored devices a check is made whether their firmware versions differ from those of the white list. If the device type and the article number of a monitored device exist in the white list, the firmware version specified in the white list for the article number is used for the validation. If monitored devices do not exist among the devices of the white list, the validation fails.	The white list can be created manually or by importing a CSV file. The expected format of CSV files is described in the section below this table. Devices can be specified with their device type or their article number. If more than one firmware version is specified for a device these must be separated by a comma. For the validation, the firmware versions detected from the specified firmware versions are used. If the check box “Ignore devices without a firmware version” is enabled, monitored devices without a firmware version detectable by the SINEMA Server have no influence on the result of the validation.	The monitored devices whose firmware versions differ from the white list are listed based on their device information. Their detected firmware versions are highlighted in red.
Different firmware versions	For all monitored devices a check is made whether devices with the same device profile or of the same device type have different firmware versions.	You can select whether the validation is performed for devices with the same device profile or devices of the same device type. If the check box “Ignore devices without a firmware version” is enabled, monitored devices without a firmware version detectable by the SINEMA Server have no influence on the result of the validation. If the “Ignore standard profiles” check box is enabled, the validation for standard profiles or the device types they contain is not performed.	The following data is specified per device profile or device type: • Number of different detected firmware versions. • Listing of these detected firmware versions • Number of devices involved

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
IP address parameters	A check is made whether there are currently monitored devices whose IP addresses, subnet masks and gateways do not match the information specified for the validation.	IP address ranges with the relevant subnet mask and gateway can be specified. Per row, an IP address and a subnet mask must be specified. If no gateway is specified, no validation is made. If a gateway is specified, this gateway must match the devices belonging to it. As an alternative to manual specification of the IP address range the IP address ranges configured in “Administration > Discovery > Scan” can be used. In this case, the subnet masks for the relevant IP address ranges must be added manually.	The monitored devices whose IP address parameters do not match the information specified for the validation, are listed based on their device information. The deviating parameters are highlighted in red.
Device names	A check is made whether there are currently monitored devices whose PROFINET device names and/or system names do not match at least one of the name patterns specified for the validation.	The name pattern of the required PROFINET device names and system names can be specified in the form of regular expressions. The information specified for the validation is not case sensitive. For PROFINET device names and system names, a maximum of 10 regular expressions can be specified. It is possible to specify whether the PROFINET device name or the system name of a device needs to match the regular expressions or whether there must be a match with the PROFINET device name and system name. The following regular expressions have no effect on the validation: • \g • \k • \l • \p	The monitored devices whose PROFINET device names and/or system names do not match the regular expressions specified for the validation are listed based on their device information. The deviating names are highlighted in red.

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Duplicate IP addresses	A check is made whether there are duplicate IP addresses in the network. Note: The detection of duplicate IP addresses is possible only if the following requirements are met: • The "Duplicate IP detection" check box is set in "Administration > Monitoring > General". • The component "Win10Pcap" was installed during installation of SINEMA Server. • To be able to detect duplicate IP addresses of NAT devices, SINEMA Server must be located in the same subnet as the NAT devices (internal subnet). Only the internal IP addresses of the devices are taken into account.	No configuration is necessary. A search is made for duplicate IP addresses starting with all network adapters of the management station.	The devices whose IP addresses occur more than once are listed based on their device information. IP addresses are highlighted in red.

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Duplicate MAC addresses	A check is made whether there are duplicate MAC addresses in the network. Detection of duplicate MAC addresses for NAT devices: • SINEMA Server is located in the external subnet: In each case, the external and the internal MAC addresses of the NAT devices are compared with each other. If one of the two MAC addresses for a NAT device does not exist, no comparison is made for this NAT device. The comparison only takes place between NAT devices. • SINEMA Server is located in the internal subnet: The internal MAC addresses of all devices are compared with each other. The comparison is made between all devices of the subnet.	No configuration is necessary. A search is made for duplicate MAC addresses starting with all network adapters of the management station.	The devices whose MAC addresses occur more than once are listed based on their device information. MAC addresses are highlighted in red.

Expected format of CSV files

A white list can be created in a text editor as a CSV file and then imported into SINEMA Server. To be able to do this, the CSV file must have the following format:

- The separator between different points of a day to record is the comma.
- Each data record is noted in a row.
- At the first position of a data record, the character string “ArticleNumber” or DeviceType” is specified. This information categorizes the information at the second position.
- At the second position of a data record, the actual article number or the actual device type is specified.
- At the third to nth position of a data record, the firmware versions are specified.

PROFINET

In the "PROFINET" category, the following validations can be configured:

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Duplicate PROFINET device names	A check is made whether there is more than one PROFINET device name per subnet of the network.	No configuration is necessary. A search is made for duplicate PROFINET device names starting with all network adapters of the management station.	The devices whose PROFINET device names occur more than once are listed based on their device information. The PROFINET device names are highlighted in red.
PROFINET IO devices without an assigned controller	A check is made whether there are PROFINET IO devices for which PROFINET monitoring is enabled and that are not assigned to a controller.	No configuration is necessary. A search is made for PROFINET IO devices without unassigned controller starting with all network adapters of the management station.	The PROFINET IO devices without an assigned controller are listed based on the device information.

Performance (devices)

In the “Performance (devices) category, the following validation can be configured:

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Device availability	A check is made for all monitored devices whether their availability in the specified period was below the specified limit value. The validation is performed only for devices on which the necessary information for the validation exists.	The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. The limit value for the availability is specified as a percentage. The default is 95%.	The monitored devices whose availability is below the specified limit value are listed based on their device information. The availability value is highlighted in red. The number of unavailable devices is also displayed.

Performance (LAN ports)

In the “Performance (ports)" category, the following validations can be configured:

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Half duplex	A check is made whether there are monitored device ports in the port mode "half duplex". Only the LAN ports in operation are checked. LAN ports in operation without a detectable port mode are evaluated as errors.	No configuration is necessary.	The ports in the port mode "half duplex" are listed based on the corresponding information.
Port speed	A check is made whether there are monitored device ports that have a lower speed than the speed specified. Only the LAN ports in operation are checked. LAN ports in operation without a detectable speed are evaluated as errors.	The limit value for the speed is specified in Mbps. The default is 100 Mbps.	The ports whose speed is below the specified limit value are listed based on the corresponding information. The speed is highlighted in red.
Interface utilization	A check is made whether there are monitored device ports that had a higher receive and/or transmit utilization than that specified. Only the LAN ports in operation are checked for which port statistics were enabled in SINEMA Server.	Either only the last detected values or the values of a period that can be entered manually are used for the validation. The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. The limit value for the utilization is specified as a percentage. The default is 50%.	The ports whose receive and/or transmit utilization is higher than the specified limit value are listed based on the corresponding information. The maximum receive and/or transmit utilization is highlighted in red.
Interface error rate	A check is made whether there are monitored device ports that had a higher receive and/or transmit error rate than that specified. Only the LAN ports in operation are checked for which port statistics were enabled in SINEMA Server.	Either only the last detected values or the values of a period that can be entered manually are used for the validation. The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. The limit value for the error rate is specified as a percentage. The default value is 0%.	The ports whose receive and/or transmit error rate is higher than the specified limit value are listed based on the corresponding information. The maximum receive and/or transmit error rate is highlighted in red.

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Discarded packets	A check is made whether there are monitored device ports that discarded more incoming and outgoing packets than specified in the period specified. Only the LAN ports in operation are checked for which port statistics were enabled in SINEMA Server.	Either only the last detected values or the values of a period that can be entered manually are used for the validation. The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. The limit value is specified by the number of discarded packets. The default is 0.	The ports whose number of discarded receive and/or transmit packets is higher than the specified limit value are listed based on the corresponding information. The number of discarded receive and/or transmit packets is highlighted in red.
Attenuation reserves of POF ports	A check is made whether there are monitored POF ports whose power margin is outside the specified range. Only the POF ports in operation are checked for which port statistics were enabled in SINEMA Server and for which information on the power margin exists. POF ports in operation without detectable values are evaluated as errors.	The range of the permitted power margin can be specified in dB. The default range is 4.5 to 99 dB.	The POF ports whose power margin is outside the specified range are listed based on the corresponding information. The power margin is highlighted in red.
Length-dependent power margin of POF ports	A check is made whether there are monitored POF ports whose attenuation reserve is outside the range specified for the cable length. Only the POF ports in operation are checked for which port statistics were enabled in SINEMA Server and for which information on the power margin exists. POF ports in operation without detectable values are evaluated as errors.	Ranges for cable lengths can be specified in m. These ranges can be assigned ranges for permitted power margin in dB.	The POF ports whose attenuation reserve is outside the range specified for the cable length are listed based on the corresponding information. The power margin is highlighted in red.

Events

In the “Events" category, the following validation can be configured:

Validation	Description of the validation	Configuration options	Presentation of the result in the PDF file if the validation did not pass.
Network events	A check is made whether more network events were triggered than specified from the selected event classes and from overall status groups if selected in the specified period.	The period stretches from the current point in time into the past. It can be specified in days, hours and minutes. The maximum permitted period is 4 weeks. If no event classes were selected, the events of all event classes are checked. You can configure whether all events or only the events of selected overall status groups are checked.	The following data is specified per overall status group: • Number of events of the event class “Error” • Number of events of the event class “Warning” • Number of events of the event class “Information”

4.3.6 Historical data and trend charts

Within the Web pages for the report types "Availability", "Performance”, “Inventory" and "Events" you can call up the recorded data and trend charts. This information is shown in additional Windows.

Select a row in the table view of a report and select one of the following menu entries using the right mouse button:

- Show historical data
- Show trend charts

Note

Show historical data

In the tables of the reports, SINEMA Server provides an additional column "Historical data". This column indicates the existence of historical data.

4.3.6.1 Historical data

Meaning

The data of a device or an interface monitored in SINEMA Server is subject to change. SINEMA Server records these changes and shows them in the historical data.

Content

For the selected report entry of a device or an interface, the displayed table "Data history" has a row for each registered change. A row contains the following entries:

Entry	Meaning
Attributes	Names the property whose status has changed. The following is displayed depending on the selected report type and the selected entry: • For devices: – IP address – MAC address – Device type – Device category – PROFINET device name – Monitoring status • For interfaces: – Interface type – Transmission rate – Interface mode
Old value	Shows the value prior to the registered change.
New value	Shows the value after the registered change.
Time of the change	Date and time of the status change

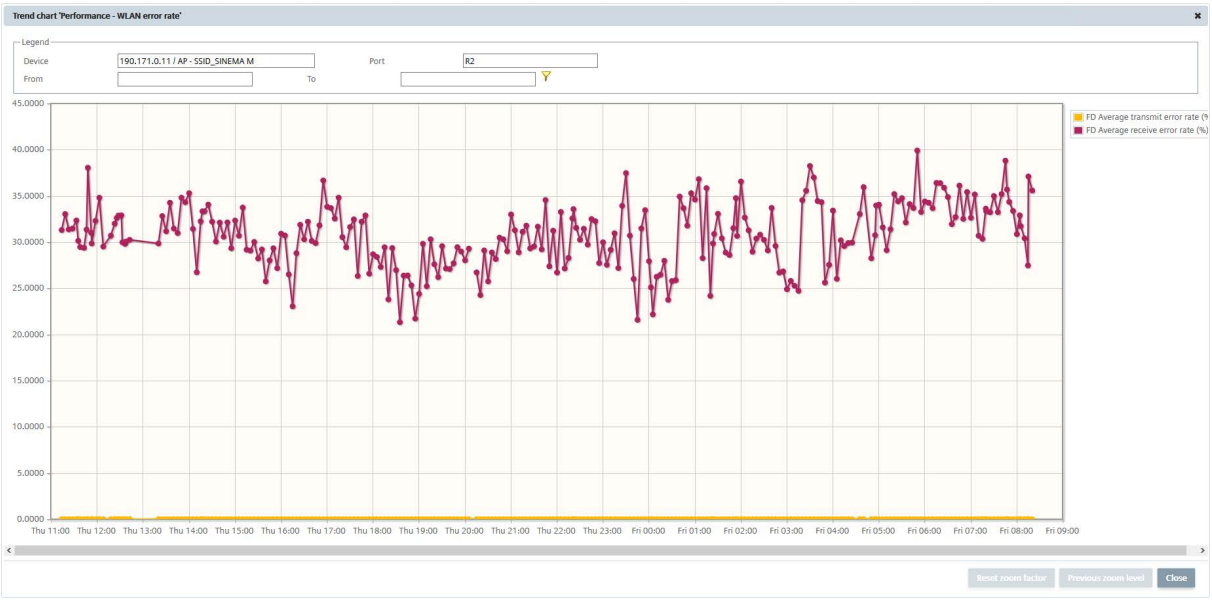
4.3.6.2 Trend charts

Meaning

Trend diagrams show certain properties of devices, interfaces and transfer parameters over time in a graphic form.

Display and content

The following figure shows the example of a possible trend chart from the "WLAN interface error rate (%)" report type with the trend of the "Average transmit error rate (%)" and "Average receive error rate (%)".



In the header, you enter a display period and enable this by clicking the filter icon.

Information on the display:

- The lines of the trend have dots that mark the end of a period. By selecting the dot with the mouse pointer, you display information about the date, time and duration of the period.
- The Y axis represents the range of values of the displayed trends data.
- The X axis represents the period of time.
- If different trend data is displayed in a chart, the color distinguishes the type of data.
- If there are interruptions in a chart line, this means that there were periods in which there was no monitoring.

Reports with trend charts

The following list shows which reports record which trend data.

Report type	Tab	Trend data
Availability	Devices	Availability in %
	Interfaces	Active time in %

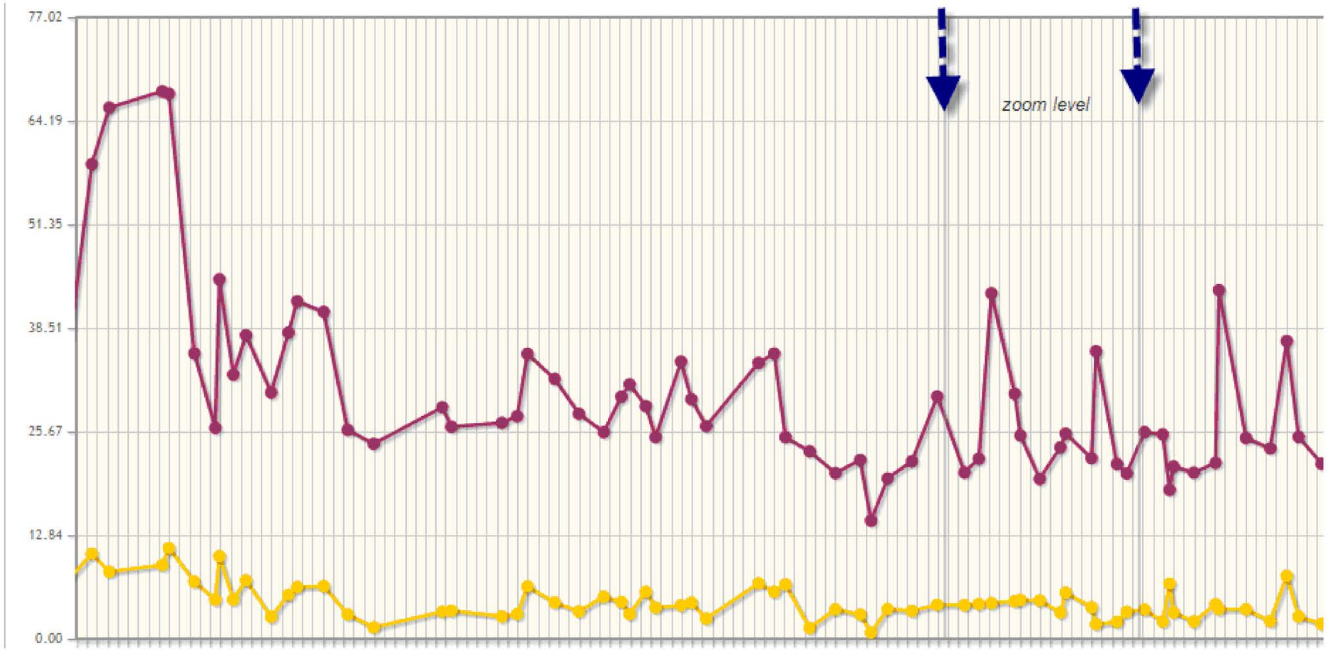
Report type	Tab	Trend data
Performance	LAN - interface utilization	• Average transmit utilization in % • Average receive utilization in % • Average utilization as % For full duplex mode, the display has 3 trend lines.
	LAN interface error rate	• Average transmit error rate in % • Average receive error rate in % • Average error rate in % Display with 2 trend lines.
	WLAN interface error rate	• Average transmit error rate in % • Average receive error rate in %
	WLAN - Interface data rate (transmission speed)	Average transmit data rate (Mbps)
	WLAN - signal strength	Average signal strength (dBm)
	WLAN - number of clients	Average number of clients

Zoom function

The zoom function of the trend charts allows you to restrict the displayed period. This increases the resolution of the display and improves the clarity of the displayed times.

To use the zoom function, follow the steps below:

1. In the trend chart, click on the required starting time of the period and hold down the mouse button.
2. Drag the mouse pointer to the required end time and release the mouse button.



4.4 Administration

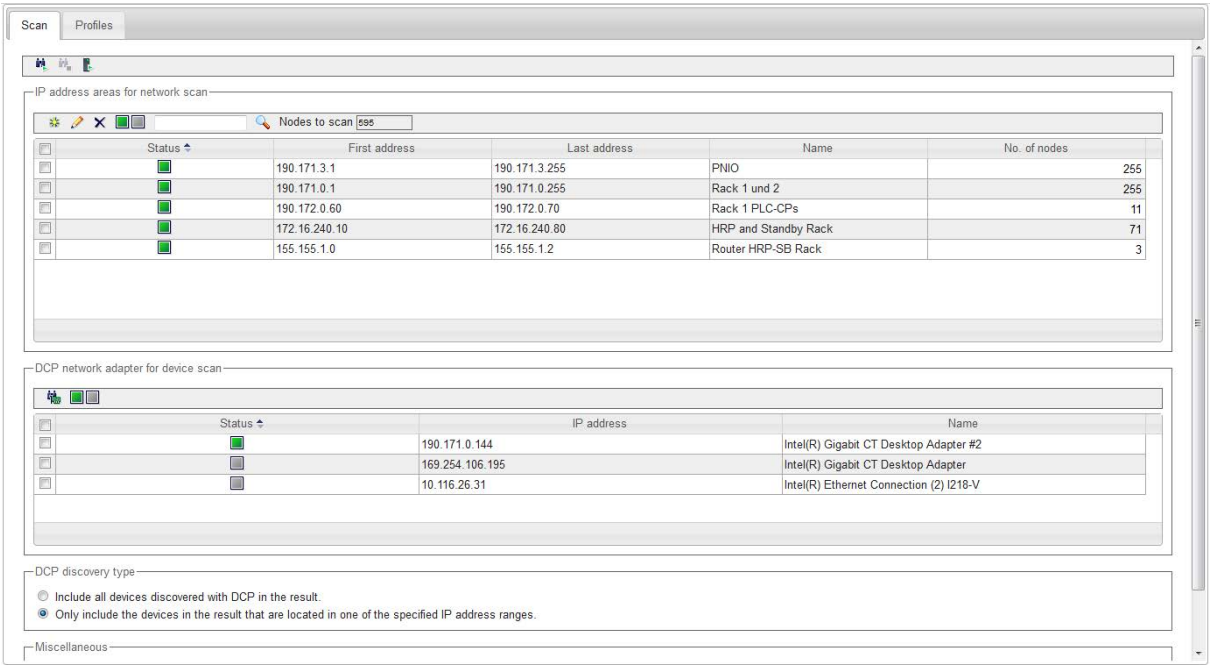
SINEMA Server includes various tools for managing the network, program, users and other objects. You can open the tools in the following Web pages using the menu commands with the same names:

"Administration > ..."

- Discovery
- Monitoring
- Events
- User
- System
- My settings
- Jobs

4.4.1 Administration - Discovery / Scan

The functions described below are available with the menu command: **"Administration > Discovery"** "Scan" tab



Scan

On this Web page, you set the parameters for the network scan and start the scan.

You have the option of specifying the IP address range for the scan in the network and the DCP network adapter of the management station used for the scan.

Other setting options relate to whether or not detected devices are taken into account and the execution of the scan.

- **Header area**

  The following table shows the function elements of the header area.

Icon	Display / function
	Start network scan When a scan is running, you can recognize this due to the appearance of the scan icon in the status bar of SINEMA Server.
	Stop network scan
	Starting automatic device type change A search is made for more suitable device profiles and device types included in them for devices that were assigned a standard profile.

- **IP address areas for network scan**

  Here you specify which IP addresses SINEMA Server should limit itself to for the network scan. With the green status icon, the corresponding range will be included in the scan, and all else excluded.

  The following table shows the functional elements of the header.

Icon	Display / function
	Create a new address range Note: A maximum of 100 IP address ranges can be created.
	Change address range
	Delete address range
	Change the status of the selected (✓) ranges green: Network range is included in the scan. gray: Network range is defined but not included in the scan.

- **"DCP network adapter for device scan" area**

  Here you specify the LAN interface of the management station to be used for the DCP network scan (green status icon).

  Note
  Restart after changing the network adapter configuration on the management station

  After changing the IP address of a network adapter on the management station, proceed as follows:

  1. Delete the management station from the device list and start a new network scan.
  2. Renew the HTTPS certificates used and then restart the PC.

  Note
  Network adapters without DCP capability

  The following network adapters cannot send DCP packets and are therefore not shown in the list "DCP network adapter for device scan".

  - CP 1604
  - CP 1616
  - CP 1616 onboard
  - CP 1613
  - CP 1613-A2
  - CP 1623
  - CP 1626
  - CP 1628

  Note
  Network scan via other protocols

  The network scan via other protocols is performed regardless of the settings configured in this area.

  The following table shows the functional elements of the header.

Icon	Display / function
	Scan LAN interfaces
	Change the status of the selected (✓) interfaces green: Network adapter is used for the scan.

- **"DCP detection type" area**

  To take discovered devices into account, select from the following options:

  – Include all devices discovered with DCP in the result.

  – Only include the devices in the result that are located in one of the specified IP address ranges.

  Note

  Effect of the option "Include all devices discovered with DCP in the result"

  If you select the option "Include all devices discovered with DCP in the result" in the DCP scan settings, note the following:

  With this setting, it is possible that DCP devices that are outside the IP ranges but within the subnets connected to the NICs are also detected.

- **"Miscellaneous" area**

  – Automatic scan

    If this check box is selected, the network scan is started automatically at the set interval. You set the interval with the **"Administration > Monitoring > General"** menu command.

  – Discovery of NAT routers: Enable this check box so that NAT routers and NAT devices are correctly detected during the network search. Enabling the check box increases the time taken for the network search depending on the network constellation. This setting does not influence the monitoring of NAT routers and NAT devices. If it is not known whether there are NAT routers in the network, the check box should be enabled and the longer time for the network search must simply be accepted.

Adapting the scan range

If you do not adapt the scan range, the device scan can take a very long time if there is a very large scan range. If the scan range covers more than 1000 addresses, a message will warn you to expect the scan to take a long time. You should therefore restrict the scan range to the devices to be monitored. To do this, it is advisable to create smaller scan groups if the IP addresses are not consecutive. This division speeds up scanning of the devices. A maximum of 100 scan groups can be created.

See also

Port settings (Page 32)

Detecting devices in the network (Page 49)

4.4.2 Administration - Discovery / Profiles

The functions described below are available with the menu command: **"Administration > Discovery"** "Profiles" tab

Displaying and editing profiles

The "Profiles" tab shows the device profiles that exist in SINEMA Server in the form of a table. Via this table, you have access to all the functions of profile editing.

You can edit the displayed profiles or add new profiles. The following types of profile must be distinguished:

- General profile

  This profile type contains information required for discovery and monitoring of network devices.

- Monitoring profile

  This profile type contains information that is only required for monitoring network devices.

  In addition to the general profile, a device can also be assigned a monitoring profile. As result, user-specific monitoring rules remain unaffected by changes in the general profile. This is an advantage when a vendor-specific general profile is replaced by a new profile version.

This difference is shown in the selectable table column Profile type.

Controlling the profile display and editing profiles - function elements

The following table explains the function elements of the header area.

Icon	Display / function
	Create new profile • Requirement: A general profile must be selected. • The Profile editor is opened with the "Add profile ID" dialog.
	Create new monitoring profile • Requirement: A general profile or monitoring profile must be selected. • The Profile editor is opened with the "Add profile ID" dialog.
	Edit selected profile • The Profile editor is opened with the "Profile" dialog with the selected profile data.
	Delete the selected profiles • Profiles are deleted following a further prompt for confirmation. • Default profiles cannot be deleted.
	Enable / disable selected profiles • Enabled profiles are used during discovery and scanning.
	Save modified profiles • The profiles marked with "*" are stored in SINEMA Server.
	Restore selected profiles • The function can be used with the profiles supplied with SINEMA Server following modification

Icon	Display / function
	Export profiles • The selected profile data is added to a ZIP archive. You are prompted to specify a storage location for downloading the ZIP archive. Before exchanging device profiles between different SINEMA Server instances, refer to the recommendations in the section Central configuration of device profile data (Page 40).
	Import profiles The dialog box for selecting the profile file is displayed. • File type: ZIP file Before exchanging device profiles between different SINEMA Server instances, refer to the recommendations in the section Central configuration of device profile data (Page 40).
	Enter text for text search / filter setting
	Start profile search Result: The profiles that contain the specified text string in one of the displayed columns.

See also

Profile concept (Page 53)

4.4.2.1 The Profile editor

Displaying and editing profiles

With the Profile editor, you can perform one of the following actions:

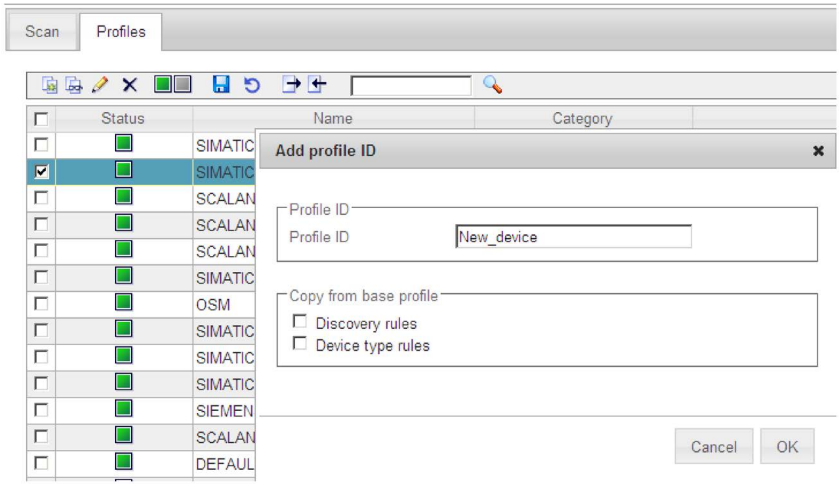
- Add a new device type to an existing profile
- Create a new profile
- Edit / modify an existing profile

The dialogs and tabs are described below.

For information on the procedure, you should also refer to the section Setting up profiles and assigning device types (Page 56)

Create new profile

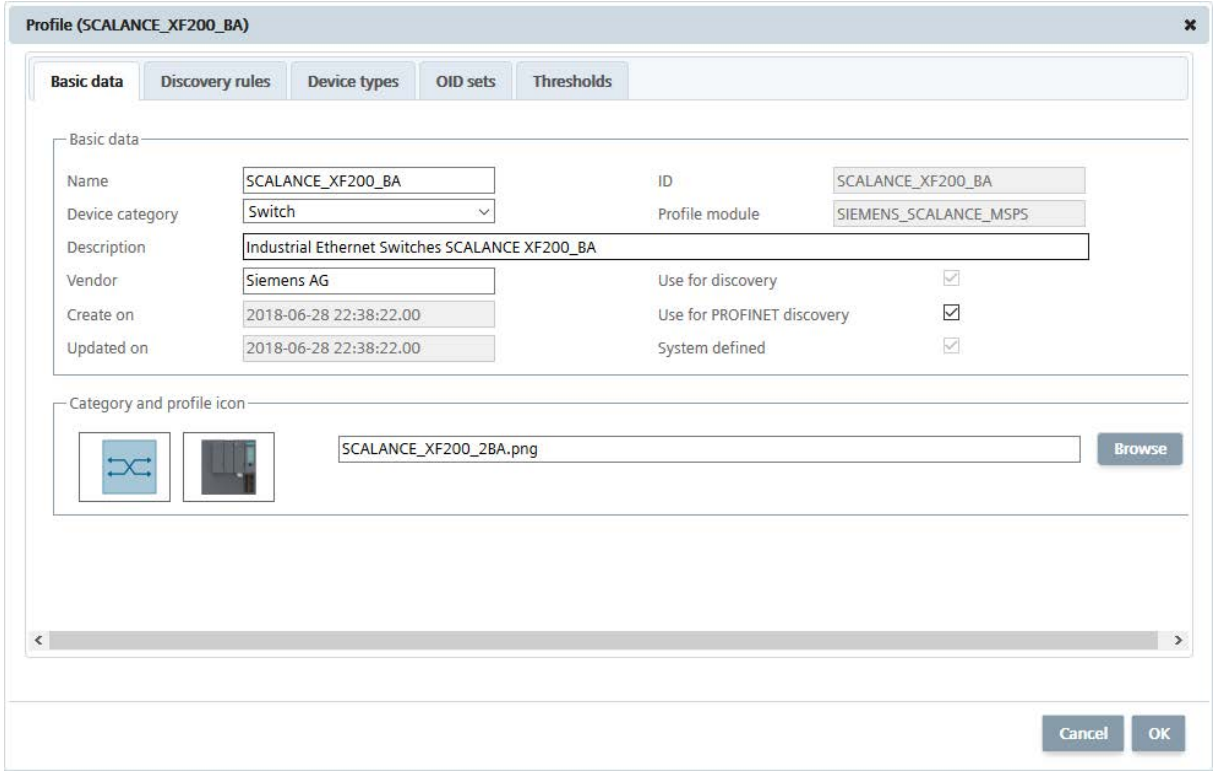
If, after selecting a profile as template, you create a new profile with the "Create profile" function element, you open the "Add profile ID" dialog.



When you confirm your entries with OK, you open the following dialogs of the Profile editor.

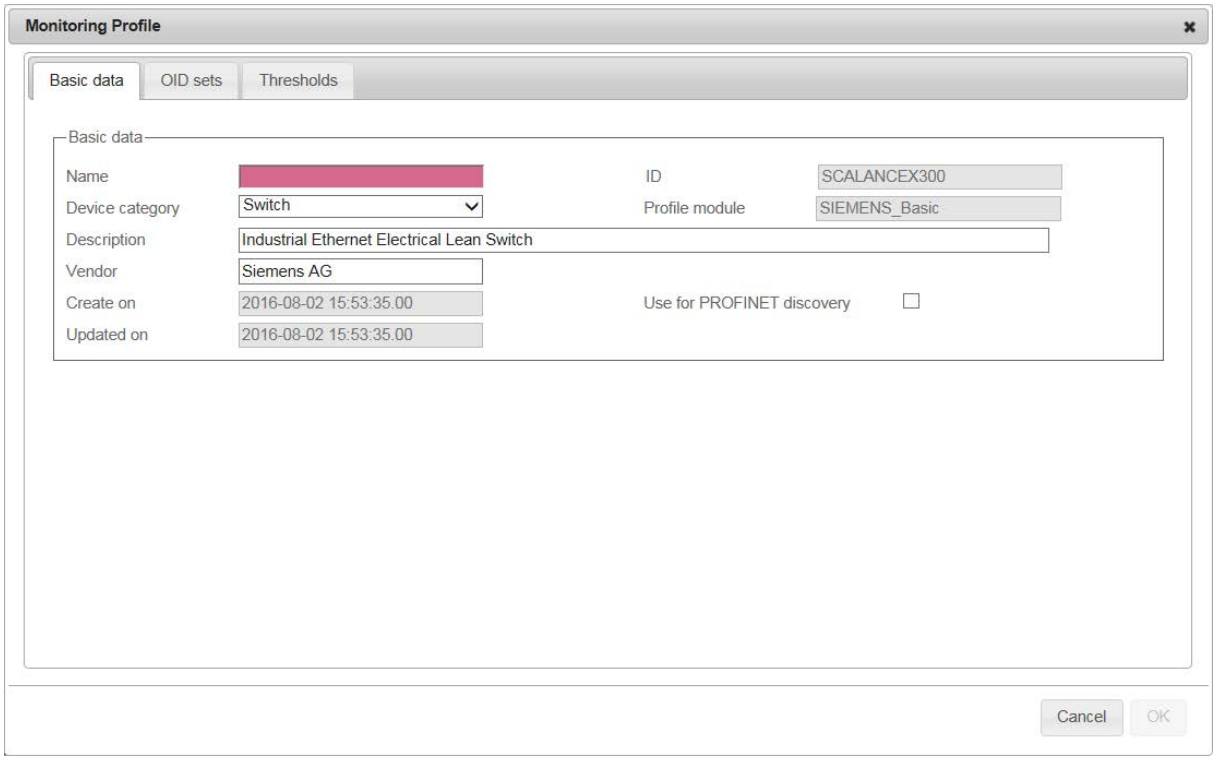
General profile - entering profile details with the Profile editor

If you edit or create a general profile, you open the dialog with the tabs required for discovery and monitoring of a network device.



Monitoring profile - entering profile details with the Profile editor

If you edit or create a new monitoring profile, you open the dialog with the tabs required for monitoring a network device.



Function elements

Some of the tabs described below also have function elements available. For information on the entries, refer to the tabs described below.

Icon	Display / function	Icon	Display / function
	Add an entry You open a further input dialog.		Edit selected entry You open a further input dialog.
	Delete selected entry The selected entry is deleted (only after you have confirmed this).		Change between "Use for discovery" / "Do not use for discovery" SINEMA Server only assigns devices to those profiles for which the setting "Use for detection" is enabled. Devices that cannot be assigned to any profiles are not monitored by SINEMA Server. For more information, refer to section Profile concept (Page 53).
	Enter text for text search / filter setting		Start search for entry Result: The entries that contain the specified text string in one of the displayed columns are displayed.

"Basic data" tab

Input box / parameters	Description
Name	Profile name
Device category	Categorization of devices of this device profile If the "Device category" device icon style is selected in the topology settings, the selection of the device category determines the icon with which devices of this device profile are displayed in the topology representations.
ID	Profile ID
Profile module	Display of the family name. The entry cannot be changed here. The entry is relevant if you want to modify the monitoring profile of the device. The monitoring profile of a device must always belong to the same profile module as the general profile.
Description	Option for entering a profile description.
Vendor	Vendor name (can be entered). Note: If a device is assigned a profile without a vendor ID, the DCP ID is used to identify the vendor.
Use for discovery	When this check box is selected, the profile is used for the device discovery.
Use for PROFINET discovery	When this check box is enabled, devices can be assigned to this device profile and the device types contained can be assigned using article numbers. By enabling the check box device profile and device type rules are activated for this device profile that contain the article numbers of the devices identifiable via PROFINET as assignment criteria. After enabling the check box in the "Criteria" area, the article numbers of device type rules can be edited. The corresponding device profile and device type rules are then updated automatically.
System defined	When this check box is enabled the profile is set by the system and was not created by the user. System-defined profiles can be reset to the factory settings and restored after deleting. The setting cannot be changed.
Device category and standard profile icon	Icon of the selected device category and selected default profile icon You can specify in the topology settings which of these two icons is used for the device display in the topologies. The device category icon is used when the "Device category" option is selected in the topology settings. The default profile icon is used when the "Device profile" option is selected in the topology settings and no suitable icon was found for the respective device type. In the overview of the device details, the default profile icon or the icon of a matching device type is always used. The assignment of icons to device categories cannot be adapted.
Created on	Date and time the profile was created
Updated on	Date and time of the last update of the profile.

"Discovery rules" tab (only for general profile)

The tab contains all the rules to be checked through during assignment of devices to device profiles.

The table must contain at least one rule to be able to enable the profile for monitoring.

Each rule must be unique within a management station and may only occur once.

The entries are made in an additional dialog. Use the function elements described above to create a new data record.

Discovery rules for the PROFINET discovery using article numbers are derived from device type rules and cannot be changed in the "Discovery rules" tab. Such discovery rules can be edited by editing the article numbers in the "Criteria" area of device type rules. The corresponding device profile and device type rules are then updated automatically.

Input box / parameters	Description
Status	Display of the status selected in the header or in the dialog. green: Rule is used for discovery.
Name	Name of the discovery rule.
Rule	Specifying a rule with criteria for SNMP/DCP. The use of the following wild cards is possible: • * (Any number of characters including spaces) • ? (The character preceding this wildcard can not or can occur once, including spaces) • . (Exactly any one character including spaces) If the characters above are not to be used as wild cards they must follow a “\” e,g. “\?”

"Device types" tab (only for general profile)

The tab is used to define a name and an icon and to specify rules for the device type assignment that will be used for the discovered devices.

If no rule is suitable for the type of a discovered device, the profile name will be used as the name of the device type and the default icon of the profile will be used to display the device.

The entries are made in an additional dialog. Use the function elements described above to create a new data record.

Input box / parameters	Description
Status	Display of the status selected in the header or in the dialog. green: Rule is used for discovery.
Icon	Icon that will be used instead of the default icon specified in the profile.
Device type	Name of the device type
Rule name	Name of the device type rule

Input box / parameters	Description
Rule	Specifying rules with protocol-specific criteria: • PROFINET: Specifying the article numbers. Several article numbers are separated by commas. The use of wildcards (*) is not allowed. It is only possible to specify article numbers in the device type criteria if the check box "Use for PROFINET discovery" has been enabled in the "Basic data" tab. The specified article numbers are also used as device profile criteria. • SNMP/DCP: Specifies the SNMP value. The use of the following wild cards is possible: – * (Any number of characters including spaces) – ? (The character preceding this wildcard can not or can occur once, including spaces) – . (Exactly any one character including spaces) If the characters above are not to be used as wild cards they must follow a "\" e,g. "\?"
Icon name	File name of the icon used
Article numbers	Article number according to the conventions of the manufacturer

"OID sets" tab

Contains SNMP OID sets

To enter or edit the values and descriptions of the OID sets, you open an extra dialog.

The entries are made in an additional dialog. Use the function elements described above to create a new data record. Per device profile, a maximum of 90 OIDs can be created in user-defined OID sets, 30 OIDs each for the data types "Integer32", "Uinteger32" and "String". The OIDs are then displayed in the device detail tab "Expert" and "User-defined OIDs" of the corresponding devices.

Only user-specific OID sets and OIDs from the system-defined OID set "Automation" can be modified. For OIDs from the OID set "Automation", an alternative OID can be specified or a fixed display value defined. In addition to this, rules can be specified for extracting partial values from the individual OIDs. Other OID sets that are read by SINEMA Server are displayed and cannot be modified.

Input box / parameters	Description
Name	Name of the OID set
Description	Text as description

"Thresholds" tab

This tab contains limit values for monitored data. Limit values are linked to operators and, for example, trigger events if values are exceeded. You can only define new limit values for OIDs from user-defined OID sets.

Creating or editing thresholds opens the editor described below:

Table 4- 26 Editor for thresholds

Input box / parameters	Description
Name	Name of the threshold
Source	For user-defined thresholds you can select the OID to be checked from a user-defined OID set. For system-defined thresholds there is no selection option.
Data type	Data type of the threshold The data type selected here decides the operators that can be used for the check. For system-defined thresholds there is no selection option.
System defined	Check box is enabled: It is not possible to create new value checks. The values and events of existing value checks can be adapted. Check box is disabled: It is possible to create new value checks. All the values and events of existing value checks can be adapted.
Overall status group	Selection of the overall status group from where the triggering event originates.
Use binary format for the threshold check	When this check box is enabled, integer values to be checked are interpreted as binary values. In the "Values" area the match with bit patterns can be checked, that are specified as follows: • Order of notation: LSB (from right to left) • Usable characters: 0, 1, ?. The placeholder ? allows both binary values. • Maximum length: 32 characters • Leading 0 do not need to be noted • The bit pattern must not only contain the placeholder ?. The check box can only be enabled if "Integer" was selected as the data type.
"Values" area	In this area you specify value checks with the aid of operators and events that should be triggered when check conditions are met.

With the button of the "Thresholds" tab, system-defined thresholds can be copied to other device profiles. Copying is only possible when thresholds with the same names exit in the target profiles. If a threshold to be copied, does not exist in the target profile, this threshold is skipped during copying. User-defined thresholds cannot be copied to other device profiles. A maximum of 10 system-defined thresholds can be copied to a maximum of 10 target profiles.

4.4.3 Administration - Monitoring

Overview

The functions described below are available with the menu command: **"Administration - Monitoring"**

The Web page contains the following tabs:

- General
- SNMP settings
- Polling groups
- OPC

4.4.3.1 Administration - Monitoring General

Administration - Monitoring General

In this tab, you configure general monitoring settings. Changes are saved with the button.

Time settings

- Scan interval
  The time interval for the automatic network scan.
- Device type change interval
  At the specified interval, a search is made for more suitable device profiles and device types included in them for devices that were assigned standard profiles.
- DCP query interval
  Specifies the time between DCP queries in seconds, assuming DCP query retries were specified.
- DCP query retries
  Number of retries for DCP queries after a device has not responded to the first DCP query. After this, the device receives the overall status "Not Reachable". If this is an alternating device, it receives the status "Not connected".
- ICMP (ping) retries
  Number of retries for ICMP queries after a device has not responded to the first ICMP query. After this the device receives the overall status "Not Reachable" or "Not Connected".
- ICMP (ping) timeout
  Specifies the time in seconds after which an ICMP query is counted as having failed.
- ICMP (ping) interval
  Specifies the time between ICMP queries in seconds, assuming ICMP retries were made.
- PROFINET reachability retries
  Number of retries for PROFINET reachability queries after a device has not responded to

the first query. A device is counted as not reachable via PROFINET after the set number of retries.

General settings

- Duplicate IP address detection
  If this check box is selected, SINEMA Server checks whether the IP address exists more than once in the network.

  Note

  Requirement for discovery of duplicate IP addresses

  The discovery of duplicate IP addresses is only possible if you have also installed the "Win10Pcap" component.

- Automatic device type change
  If this check box is selected, a search is made for more suitable device profiles and the device types in them for devices that were assigned standard profiles. The default interval for automatic device type change is 70 minutes and can be configured in the "Time settings" area. In addition to this, the automatic device type change is always performed when a device with an assigned standard profile changes from the "Not reachable" status to the "Reachable" status.
- Detect alternating devices automatically (based on the Fast Startup function of the devices)
  When this check box is enabled, devices that support the "Fast Startup" function are automatically detected by SINEMA Server as alternating devices when they start up and included in the monitoring.
- Learn connections of alternating devices automatically
  When this check box is enabled, SINEMA Server learns all connections of alternating devices and shows these in the topology display. Learned connections are historical connections that remain displayed after they have been terminated.
  - Automatically configure ports with several learned connections as docking ports (can only be selected when the "Learn connections of alternating devices automatically" check box is also selected)
    When this check box is selected, SINEMA Server automatically configures ports with more than one learned connection as docking ports.
- Consider duplicate PROFINET device names in topology

  Select this check box if duplicate PROFINET device names are located in the network and the devices are to be displayed in the topology view.
- Permanently disable LAN port statistics for all monitored devices
  When this option button is enabled, no port statistics of LAN ports are monitored, not even for newly detected devices. The setting cannot be changed manually for individual LAN ports.

- Permanently enable LAN port statistics for all monitored devices
  If this option button is enabled, information about data traffic, port load and error rates is monitored using SNMP or possibly PROFINET for the LAN ports of all monitored devices. If devices are newly discovered and monitored, the port statistics for their LAN ports is enabled automatically. The setting cannot be changed manually for individual LAN ports.

  Note

  For gigabit ports with SNMP V1 monitoring, port statistics cannot be enabled due to the protocol.

  Note

  Enabling port statistics for all LAN ports can lead to high network load.

- Configure LAN port statistics manually for all monitored devices
  The current settings for LAN port statistics are retained and can be changed manually for the individual ports.
  When selecting this option box, you can optionally select the following check box:
  – Disable LAN port statistics for all monitored devices once
    If this check box is selected, the LAN port statistics for all monitored devices are disabled. The settings for the LAN port statistics can then be changed manually for the individual ports.

PROFINET discovery and monitoring settings

With the PROFINET discovery settings described below, you can exclude devices from PROFINET discovery by SINEMA Server. PROFINET discovery of devices by SINEMA Server is not a requirement for monitoring them with PROFINET.

- PROFINET discovery

  If this check box is selected, PROFINET is used to detect devices.

- PROFINET discovery is not performed for the following IP addresses: (can only be selected if the check box "PROFINET discovery" is enabled)

  If this check box is selected, PROFINET discovery by SINEMA Server is not performed for the devices whose IP addresses are specified in the corresponding text box. The devices can be specified via IP addresses, IP address ranges or using CIDR notation. The entered values can be validated via the button. The IP addresses that SINEMA Server can use to access these devices must be specified for the devices.

PROFINET monitoring and PROFINET diagnostics are only supported for devices with PROFINET IO capability. The PROFINET monitoring settings listed below only affect monitored devices.

- PROFINET monitoring
  If this check box is enabled, PROFINET monitoring and PROFINET standard diagnostics as well as PROFINET channel diagnostics of PROFINET devices is enabled globally. Activating this monitoring at the device level is achieved using device parameters with the same name, see section Device window with device list (Page 96). Events relevant for diagnostics can only be triggered when PROFINET monitoring is enabled.
- PROFINET monitoring of port statistics (can only be selected when the "PROFINET monitoring" check box is enabled)
  If this check box is set, PROFINET monitoring of LAN port statistics for PROFINET devices is enabled globally. Activating this monitoring at the device level is achieved using device parameters with the same name, see section Device window with device list (Page 96)
  In addition to this, the port statistics must be enabled in the device details for the required LAN port.
- Use PROFINET monitoring settings for newly discovered PROFINET devices
  If this check box is enabled, the configuration of the two options named above is used for newly discovered devices.
- Duplicate PROFINET IO name detection
  If this check box is set, SINEMA Server checks whether or not the PROFINET IO device name exists more than once in the network.

  Note

  Duplicate PROFINET IO device names are not permitted as per the PROFINET standard.

- PROFINET diagnostics text library

  The PROFINET diagnostics text library contains all texts that SINEMA Server displays in the "Text" column of the PROFINET channel diagnostics and as details in the corresponding events. These texts can be made available to SINEMA Server by importing files in the XML language GSDML. In channel diagnostics SINEMA Server assigns the raw data read out from the devices to the texts from the PROFINET diagnostics text library. If there are no texts for the raw data, the raw data is displayed in hexadecimal format. A maximum of 10 XML files can be imported at one time. The languages supported for the texts of the PROFINET diagnostics text library are German. English, French and Chinese. The overwriting of existing entries can be enabled with the button. If texts to be imported do not exist in language, when the texts of this language are overwritten, the English versions are used. Importing diagnostics texts that were exported in the CSV format using the export function in "Administration > System > Configuration" is also possible. As default. standardized PROFINET texts and standardized texts for devices from Siemens exist in SINEMA server. Every test can be enabled, disabled or deleted in the PROFINET diagnostics text library. After disabling texts, the corresponding events are no longer triggered and the data belonging to them is not displayed in the PROFINET channel diagnostics. When a text is deleted from the PROFINET diagnostics text library, the raw data belonging to it is displayed in hexadecimal format in the PROFINET channel diagnostics and in the event details.

SIMATIC monitoring settings

Devices for which SIMATIC monitoring is supported are known in this document as being "with SIMATIC capability". These devices are listed in the Readme file. The following SIMATIC monitoring settings are available:

- SIMATIC monitoring
  If this check box is set, SIMATIC monitoring of CPUs with SIMATIC capability is enabled globally. Activating this monitoring at the device level is achieved using device parameters with the same name, see section Device window with device list (Page 96).
- SIMATIC monitoring of assigned devices (can only be selected when the "SIMATIC monitoring" check box is enabled)
  When this check box is enabled, the SIMATIC monitoring of device data about assigned PROFINET IO devices and that is available on CPUs with SIMATIC capability is enabled globally. Activating this monitoring at the device level is achieved using device parameters with the same name, see section Device window with device list (Page 96).
- SIMATIC monitoring including assigned devices and SIMATIC event messages (can only be selected when the "SIMATIC monitoring of assigned devices" check box is enabled)
  When this check box is enabled, SINEMA Server logs on to CPUs with SIMATIC capability to receive SIMATIC event messages. The received event messages are displayed in the global and in the device-specific event list of the CPU and are indicated as having the status "Incoming" (for active statuses) or "Outgoing" (for no longer active statuses). Activating this monitoring at the device level is achieved using device parameters with the same name, see section Device window with device list (Page 96)
  The logon to receive SIMATIC event messages from CPUs with SIMATIC capability can be restarted by the shortcut menu entry "Log on again for SIMATIC event / alarm messages".
- SIMATIC monitoring including assigned devices and SIMATIC alarm messages (can only be selected when the "SIMATIC monitoring of assigned devices" check box is enabled)
  When this check box is enabled, SINEMA Server logs on to CPUs with SIMATIC capability to receive SIMATIC alarm messages. The received alarm messages are displayed in the global and in the device-specific event list of the CPU and are indicated as having the status "Incoming" (for active statuses) or "Outgoing" (for no longer active statuses). Activating this monitoring at the device level is achieved using device parameters with the same name, see section Device window with device list (Page 96)
  The logon to receive SIMATIC alarm messages from CPUs with SIMATIC capability can be restarted by the shortcut menu entry "Log on again for SIMATIC event / alarm messages".

Note

Requirements for receiving and displaying SIMATIC event messages / alarm messages

To allow SINEMA Server to receive and display SIMATIC event messages / alarm messages from a CPU with SIMATIC capability, the following requirements must be met:

- In the STEP 7 configuration of the CPU, SIMATIC event messages / alarm messages must be enabled so that end devices can log on to the CPU to receive the messages. Enabling the messages for SINEMA Server is based on the same principle as for HMI devices.
- To assign the messages to message texts, the option "Enable Web server on module" must be enabled in the STEP 7 configuration of the CPU. As an alternative in STEP 7 as of V5.5.4 the option "Generate and load Web server configuration" can be enabled. This is, however, not available for all CPUs with SIMATIC capability.

For more information, refer to the Siemens Industry Online Support:
Link (https://support.industry.siemens.com/cs/ww/en/ps/13828)

See also

Alternating devices (Page 120)

4.4.3.2 Administration - Monitoring SNMP settings

SNMP settings

The following table explains the function elements of the header.

Icon	Display / function	Icon	Display / function
	Create new record for SNMP settings		Change SNMP settings
	Delete SNMP settings		Change the status of the selected (✓) SNMP settings

The table below this shows the existing data records with SNMP settings. As default, the following SNMP settings are available and enabled:

SNMP setting	SNMP version	Read community	Write community
SIEMENS IPCs with Diag-Monitor	2c	DMMCL	DMMCL
SNMP settings - V2c	2c	public	private
SNMP settings - V1	1	public	private

During the network scan, SINEMA Server searches through all devices capable of SNMP in descending order of the active SNMP versions. If an SNMP setting with version 3 is available and enabled, this setting is used by SINEMA Server during the scan.

If logging on to a device with one of the configured SNMP settings fails, SINEMA Server automatically disables SNMP monitoring for this device to prevent the device from blocking

the IP address of SINEMA Server. After correcting the SNMP settings in SINEMA Server, you can enable SNMP monitoring again in the monitoring settings of the device. The monitoring settings of the device can be accessed via the button in the advanced settings of the device window, see section Device details (Page 104).

Note

Using SNMP V3

For reasons of security, it is advisable to use SNMP settings in which SNMP V3 is used. Select only secure passwords with a high password strength.

Note

Limit number of used SNMP settings

SNMP access is blocked by some devices after 10 failed authentication attempts. You should therefore only use a limited number of SNMP settings.

Note

Receipt of SNMP traps by SINEMA Server

SINEMA Server cannot process SNMP notifications as Informs. If SNMP V3 is selected as diagnostic protocol, it must be ensured that notifications are sent as (SNMP V1) traps. This is a device setting that must be made accordingly on each SNMP V3 network device. If the notifications are not sent as traps, SINEMA Server cannot receive/display these or consider them during device diagnostics.

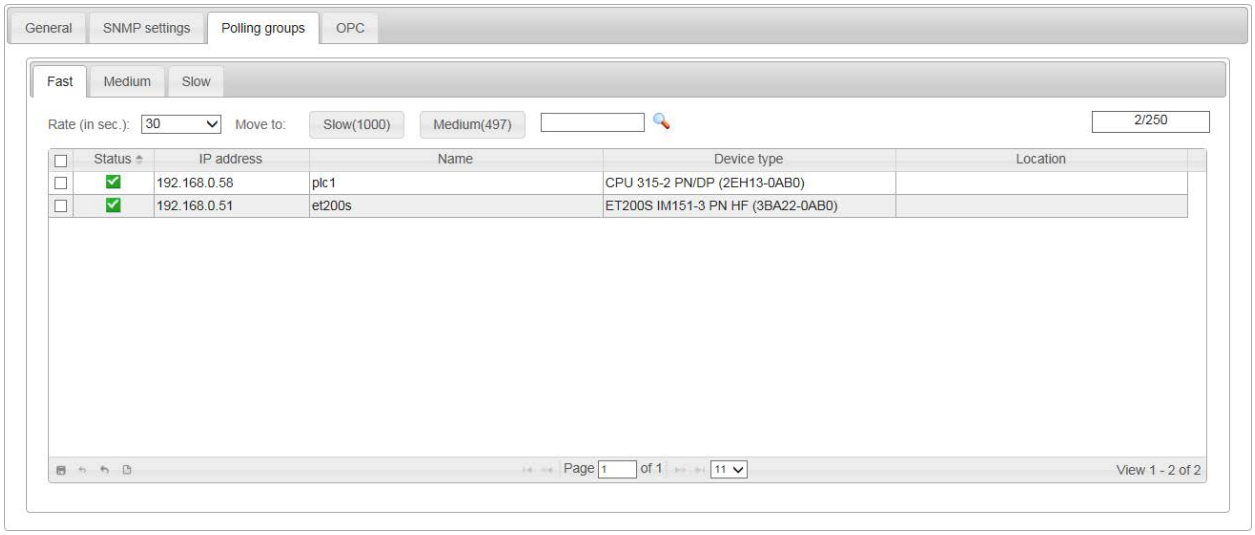
Depending on the SNMP version (1, 2c, 3), when you create or change a record, another window opens in which you can enter the parameters of this version, for example

- Retries
- Timeout
- Security level
- User name
- Authentication algorithm
- Authentication password
- Encryption algorithm
- Encoding password

When a password is entered, the current password strength is checked. You can find the criteria for determining the password strength in the section Password strength (Page 238).

4.4.3.3 Administration - Monitoring Polling groups

This window shows the three polling groups "Fast", "Medium" and "Slow" each in a separate tab, together with their assigned network devices.



Meaning

A polling group is a device group whose UP/DOWN status is queried at a certain interval (polling rate) via the ICMP protocol. The polling rate can be specified for each group within a certain range. The number of devices per group is limited. The division into 3 polling groups is defined for the relevant bandwidth of their polling rate. The following groups are distinguished

- Fast
- Medium
- Slow

Network devices that are not monitored or that can be ignored or are classified as non-critical can be moved to lower-level polling groups. This means that such devices are polled at a longer interval. This technique allows you to control the network load when lots of devices need to be polled.

Polling groups

The 3 polling groups appear in the form of tabs within the polling dialog. These polling groups are divided up based on the polling rate measured in seconds.

- Fast

  This group is intended for all devices that need to be polled frequently.

  – The default setting is 30 seconds.

  – The minimum polling interval is 10 seconds; the maximum polling interval is 60 seconds.

  – As default, the group can contain up to 100 devices. Up to 250 devices can be assigned.

- Medium

  This group is intended for all devices that need to be polled with medium frequency.

  – The default setting is 150 seconds.

  – The minimum polling interval is 90 seconds; the maximum polling interval is 150 seconds.

  – As default, the group can contain up to 200 devices. Up to 500 devices can be assigned.

- Slow

  This group is intended for all devices that need to be polled less frequently.

  – The default setting is 300 seconds.

  – The minimum polling interval is 180 seconds; the maximum polling interval is 300 seconds.

  – As default, the group can contain up to 200 devices. Up to 1000 devices can be assigned.

Note

Number of devices

The number of devices shown in the medium and slow tabs is the number of devices remaining until the maximum possible number of devices is reached.

Operator input

The following table shows the functional elements of the header:

Icon	Display / function	Icon	Display / function
Rate (in sec.): 30	Polling rate in seconds	Fast (150)	Transfer selected (✓) devices to the "Fast" polling group *
Slow (120)	Transfer selected (✓) devices to the "Slow" polling group *	Medium (50)	Transfer selected (✓) devices to the "Medium" polling group *
	Enter text for text search		Start text search
41/250	Display the used / available table entries		

*) The number after the group name indicates how many table entries are still available.

The table below this shows the network devices assigned to this group, in each case with

- Status
- IP address
- Name
- Device type
- Location

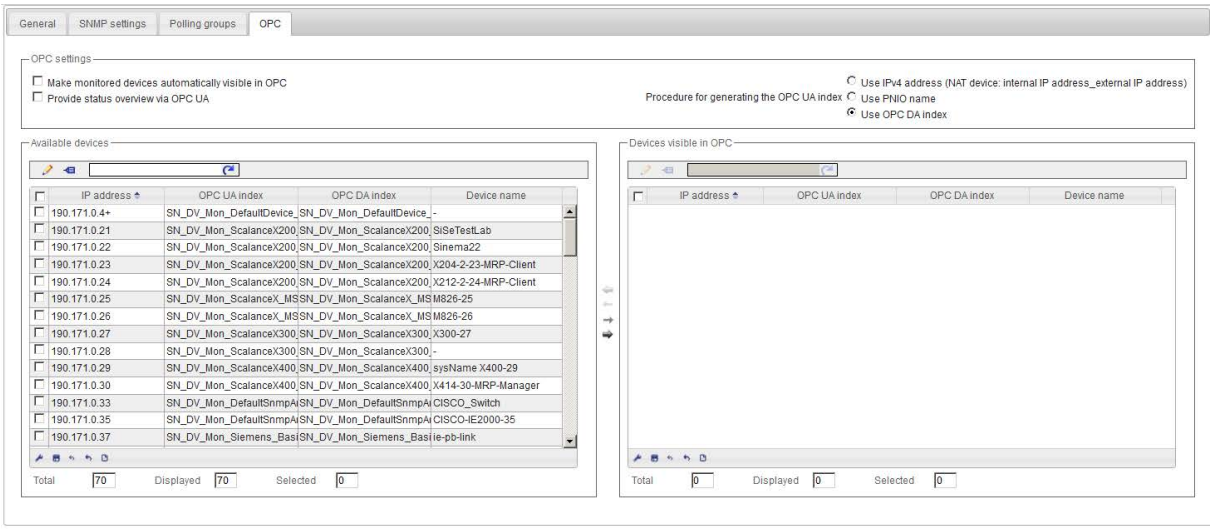
Setting up polling groups - procedure

To move devices from one group to another, follow the steps below:

1. Select the device or the devices you want to move to another group.
2. Click the appropriate icon in the header. Result: The selected devices are moved to the required group.

4.4.3.4 Administration - Monitoring OPC

You open the Web page shown below using the menu command: **"Administration > Monitoring > OPC"**



Overview

In industrial manufacturing, devices of different manufacturers with different process controllers as well as incompatible protocols and data formats are often used. For these to be able to communicate with each other, an open communications standard (OPC --> Open Process Control) was defined. This allows plant data, alarms, events and other process data to be exchanged between all systems in real time. SINEMA Server also provides the option of making data available using OPC.

For more information on the topic of OPC in SINEMA Server, see also the section Data exchange via OPC (Page 243)

Layout

In the "Administration > Monitoring > OPC" window, you can configure the data of which devices will be sent to an OPC server. This device data is then visible for OPC clients and can be evaluated and monitored by them. Device data from unmonitored and passively monitored devices cannot ever be sent to an OPC server.

OPC settings

In the dialog area "OPC settings", the following control elements are available:

Operator control element	Function
Make monitored devices automatically visible in OPC	When this check box is selected, the device data of all devices monitored by SINEMA Server is visible in OPC.
Procedure for generating the OPC UA index	For monitored devices that do not yet have an OPC UA index, SINEMA Server generates an OPC UA index using one of the following procedures: • Using the Ipv4 address The OPC UA index is formed from the four digits of the IPv4 address of the device. The periods of the IPv4 address are not adopted If the digits have less than three places, the missing places are filled out with the digit "0". Example: IPv4 address: 102.23.10.4 OPC UA index: 102023010004 OPC UA index for NAT devices: <internal IP address>_<external IP address>, e.g. 192168110237_192168111237 In the case of an IP address change, the OPC UA index is not updated. • Using the PNIO name: The PNIO name of the device is used as the OPC UA index. A maximum of 64 characters of the PNIO name are adopted. If non-permitted characters occur in the PNIO name, these are replaced by the "_" character. • Using the OPC DA index (default setting): The OPC DA index of the device is used as the OPC UA index. If this setting is changed, existing OPC UA indexes are not updated.
Provide status overview via OPC UA	When this check box is selected, the following information is provided via OPC: • The numbers of devices per overall status • The worst existing overall status • The following information is provided for each view: – Name of the view – Name of the higher-level view – The worst existing overall status – Number of reachable devices – Number of unreachable devices – Number of unconnected devices The overall states are indicated by the following values: • 1: Not reachable • 2: Error • 3: Maintenance demanded • 4: Maintenance required • 5: OK • 6: Not connected • 7: Unmonitored • 8: Passively monitored

Available devices and visible in OPC

In the dialog area "Available devices and devices visible in OPC", it is possible among other things to configure the data of which devices is visible in OPC manually. If the "Make monitored devices automatically visible in OPC" check box is selected in the OPC settings, settings made relating to this are ignored and the corresponding control elements are disabled.

The following control elements are available:

Operator control element	Function
	A dialog opens in which the OPC UA index of the selected device can be changed manually. Using the button  in this dialog, the existing OPC UA index is updated according to the configured procedure. The OPC UA index must be between 6 and 64 characters long and must be unique among the monitored devices. Spaces, tabs and the following characters must not occur in the OPC UA index: .:;,[]{}?*\/%!()$@
	Update the OPC UA indexes of the selected devices according to the configured procedure.
	Enter text for text search / filter
	Start text search / filter setting
	Remove all devices from the list "Devices visible in OPC"
	Remove all devices from the "Devices visible in OPC" list
	Add the selected (✓) devices to the "Devices visible in OPC" list
	Add all devices to the "Devices visible in OPC" list

In the footer, there is information about how many devices are in each area in total, and how many are displayed and selected.

Although the column assignment in the data area is preset, you can arrange it any way you require ( in the footer). You can choose from all the device properties as those available via the device window and the device details.

4.4.4 Administration - Events

4.4.4.1 Administration - Events Event types

The web page described below can be accessed with the menu command "Administration > Events > Event types".

Events are divided into network and system events. Network events provide information on status changes in the network or contain device traps. System events contain system-related status information of SINEMA Server.

On this page, you can by default disable existing event types of both categories, enable them and adjust their display in multiple languages. You can also create new network event types and trap types. For network events of a created network event type to be triggered, the network event type must be assigned to an overall status group and then assigned to a threshold in the profiles of the required devices; see section The Profile editor (Page 179). When creating a trap type, you must specify the OID to which the traps to be received relate.

Operator input

The following table explains the function elements of the header.

Icon	Display / function
	Create a new event type (only network event) The input dialog is displayed. If you enable the "Trap" check box, you can specify the OID that will trigger the trap network event (see representation above).
	Edit event type The input dialog is displayed (see above)
	Delete event type (only network event) Note: Network events created by "System" cannot be deleted.
	Change the status of the selected (✓) event type (activated / deactivated) Note: Deactivated event types move to the end of the table.
	Restore the default settings for selected event types Note: Event types created by "User" cannot be reset.
	Enter text for text search / filter setting
	Start text search / filter setting Result: The traps / events that match the text string specified for the text search are displayed.
	Filter the display according to the following criteria: • All • Enabled • Disabled

Content

The events are shown in the form of a table.

Although the column assignment in the data area is preset, you can arrange it any way you require (in the footer). The following information can be selected:

Parameter	Meaning
"Check box"	Select this option to select all the displayed entries.
Status	Shows the status of the events (enabled / disabled)
Text	Contains the configurable event text.

Parameter	Meaning
Class	Contains the configurable classification.
Trap OID (only with "network events")	Object identification The OID is set by the particular network device. If traps are received and the OID is unknown, the OID box in the display remains empty.
Original text	Contains the text entry specified the first time the event type was detected.
Original class	Contains the classification that was specified the first time the event type was detected.
Originator (only for "network events")	Specifies the instance that made the initial definition. The following are possible: • System • User
Overall status group	Specifies the overall status group to which the event belongs. The following are possible: • Name of the overall status group • None

Input dialog - special features

The entry in the text boxes is language specific. If you write to the text box directly, the text is stored under the currently set language.

If you click the globe symbol beside the text box, you open an additional dialog in which you can make the entries for the permitted languages.

4.4.4.2 Administration - Events Overall status groups

Function of overall status group

An overall status group is a group of functionally related events that influence the overall status of a device or the overall status of SINEMA Server. Each event within an overall status group can be assigned an overall status that the device / SINEMA Server will adopt when the corresponding event condition occurs.

Conventions for events in the overall status groups

The following conventions apply to events in the overall status groups:

- An overall status group must contain at least one event. A maximum of 20 events can be assigned to an overall status group.
- An event can only belong to one overall status group.
- Only events assigned to an overall status group can influence the overall status of a device / SINEMA Server.

Statuses of events in overall status groups

To form the overall status of devices / SINEMA Server, various statuses are significant that events from overall status groups can adopt. These event statuses are displayed in the "Event status" column of the event list.

Event status	Meaning
Pending	When an event that is assigned a negative overall status (every overall status except "OK" and "Not connected") is triggered for a device / SINEMA Server, it is given the event status "Pending". This status indicates that the event was entered in a list of pending events for the device / SINEMA Server.
Resolved automatically	An event that was removed from the list of pending events by SINEMA Server is identified by the event status "Resolved automatically". Resolved events can no longer influence the overall status of devices / SINEMA Server. Pending events are automatically resolved by the following events: • Events assigned the "OK" or "Not connected" overall status from the same overall status group • Pending events of the same overall status group (regardless of the assigned overall status)
Resolved manually	An event that was removed from the list of pending events manually using the stamp icon in the event list is identified by the event status "Resolved manually".
-	A triggered event that is not assigned to any overall status group or is not assigned any overall status in the group has no event status.

Rules for forming the overall status

The overall status of devices / SINEMA Server is formed by events from the overall status groups according to the following rules:

- The event with the most negative overall status pending for a device/SINEMA Server determines the overall status of the device/SINEMA Server. The classification as the most negative overall status applies to all the overall status groups.
- After the automatic or manual resolution of pending events, the device / SINEMA Server receives the most negative overall status assigned to one of the remaining pending events. If there is no further event pending for the device / SINEMA Server, the device / SINEMA Server receives the overall status "OK" or "Not connected".

Example of forming overall statuses

In the following example, various events are triggered by a device that belong to different overall status groups.

The overall status groups are made up of the following events:

- Overall status group "A":
  - Event "A1": Warning - Overall status "Maintenance demanded"
  - Event "A2": Warning - Overall status "Maintenance required"
  - Event "A3": Info - Overall status "OK"
- Overall status group "B":
  - Event "B1": Warning - overall status "Error"
  - Event "B2": Info - Overall status "OK"
- Overall status group "C":
  - Event "C1": Warning - Overall status "Maintenance demanded"

The following table shows the changes in the device overall status based on the occurrence of these events and the events pending for the device. Initially there are no pending events for the device and the device has the overall status "OK".

Triggered event / user action	Overall status of the device	Events pending for the device
A1	Changes from "OK" to "Maintenance demanded".	• A1 - "Maintenance demanded"
A3	Changes from "Maintenance demanded" to "OK".	None
C1	Changes from "OK" to "Maintenance demanded".	• C1 - "Maintenance demanded"
The user triggers the event status "Pending" for the event "C1".	Changes from "Maintenance demanded" to "OK".	None
A1	Changes from "OK" to "Maintenance demanded".	• A1 - "Maintenance demanded"
A2	Changes from "Maintenance demanded" to "maintenance required".	• A2 - "Maintenance required"
B1	Changes from "Maintenance required" to "Error".	• A2 - "Maintenance required" • B1 - "Error"
C1	"Error", no change.	• A2 - "Maintenance required" • B1 - "Error" • C1 - "Maintenance demanded"
A3	"Error", no change.	• B1 - "Error" • C1 - "Maintenance demanded"
B2	Changes from "Error" to "Maintenance demanded".	• C1 - "Maintenance demanded"
The user triggers the event status "Pending" for the event "C1".	Changes from "Maintenance demanded" to "OK".	None

Network groups and system groups

Network groups only contain events that can influence the overall status of devices. Events from system groups can only influence the overall status of SINEMA Server.

System-defined and user-defined overall status groups

In system-defined overall status groups, the assignments of overall statuses to events belonging to the overall status group can be adapted. Events of the overall status group can also be enabled / disabled. Existing events cannot, however, be removed from a system-defined overall status group. It is also not possible to add an event to a system-defined overall status group.
All system groups are defined by the system. No actions can be executed on system groups.

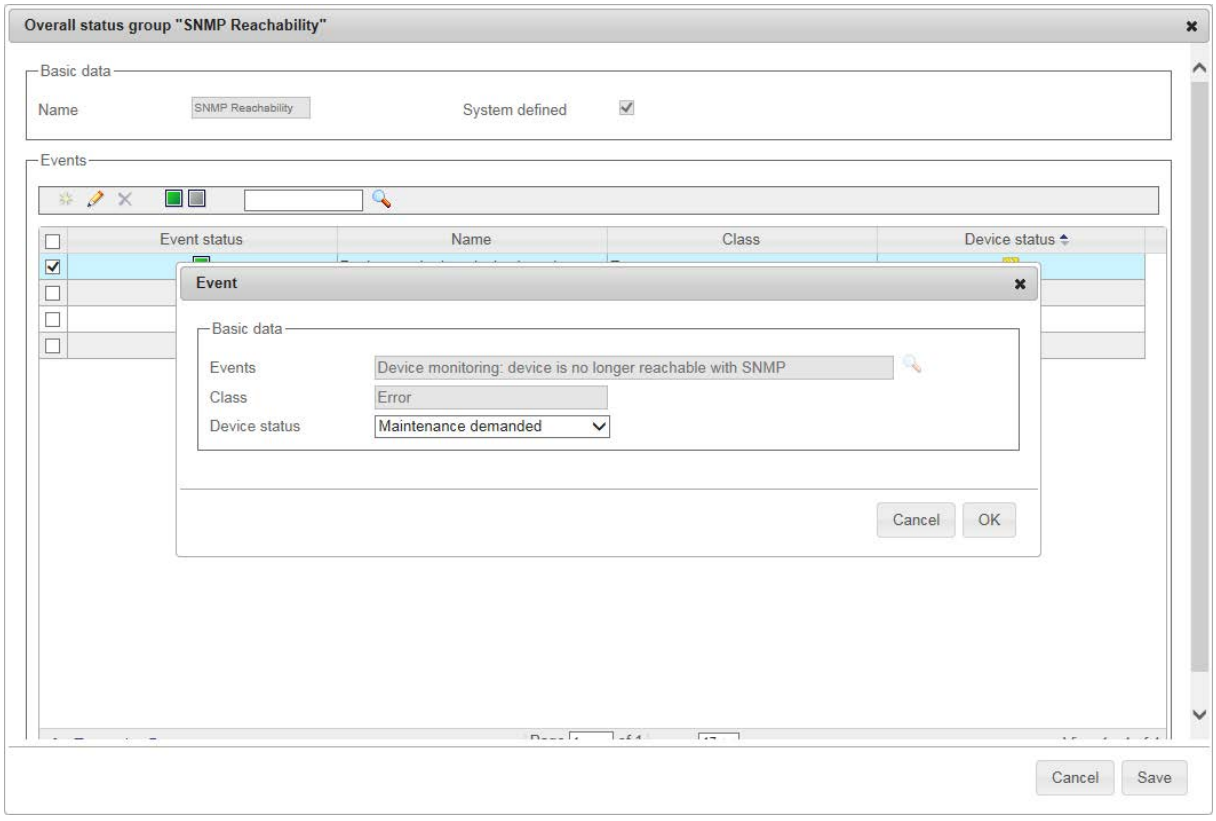
Note

System-defined overall status group "POF Power Margin - Cable length"

The events of the system-defined overall status group "POF Power Margin - Cable length" are disabled as default. If these events should be included in the device monitoring, they need to be enabled.

In user-defined overall status groups events can be included that are visible in the entry "Event types". Overall statuses can be freely assigned to these events. It is also possible to remove events from user-defined overall status groups. A maximum of 100 overall status groups can be created.

The following figure shows the events of the system-defined overall status group "SNMP Reachability" and the properties dialog of an assigned event:



Layout of the Web page

On the "Administration > Events > Overall status groups" Web page, network groups and system groups are displayed. The overall status groups can be displayed in the "System groups" tab but not edited. The following paragraphs in this section relate to the "Network groups" tab.

Operator input

The following table explains the operator controls of the header:

Operator control	Function
	Create new overall status group The dialog for configuring overall status groups is displayed (see description below).
	Edit overall status group The dialog for configuring overall status groups is displayed (see description below).
	Delete overall status group Note: System-defined overall status groups cannot be deleted.
	Reset selected overall status groups The selected system-defined overall status groups are reset to the default settings.
	Enter text for text search / filter setting
	Start text search / filter setting Result: The overall status groups that match the text string specified for the text search are displayed.

Content

The overall status groups are shown in the form of a table.

Parameter	Meaning
"Check box"	Select this option to select all the displayed entries.
Name	Name of the overall status group
System-defined	Specifies whether the overall status group is system-defined or user-defined. In system-defined overall status groups, the assignments of overall statuses to events belonging to the overall status group can be adapted. Events of the overall status group can also be enabled / disabled. Existing events cannot, however, be removed from a system-defined overall status group. It is also not possible to add an event to a system-defined overall status group. All system-related overall status groups are defined by the system. The assignment of overall statuses to events from system-related overall status groups cannot be adapted. In user-defined overall status groups, any events created in "Event types" can be included. Overall statuses can be freely assigned to these events. It is also possible to remove events from user-defined overall status groups. A maximum of 100 overall status groups can be created.

Dialog for configuring overall status groups

This dialog shows the name of the overall status group and its events. Assigned events can be enabled or disabled for triggering. User-defined overall status groups can be assigned events that are visible in the entry "Administration" > "Events" > "Event types". After selecting an assigned event or the icon  , the dialog for assigning events opens.

Dialog for assigning events

This dialog is used to select an assigned event and to select the overall status that the event will cause if it is triggered. The following functions are available:

- Event: Name of the assigned event. In user-defined overall status groups, the dialog for selecting the assigned event can be opened using the icon  . In this dialog, you can select the network event to be assigned. The OIDs are displayed as default in the selection dialog for trap network events.
- Event class: Categorization of the assigned event.
- Overall status: Overall status that the event will cause if it is triggered.
- OID: Display of the OID of a selected trap network event.

4.4.4.3 Administration - Events > Event reactions

The dialogs described below can be accessed via the menu command "Administration > Events > Event Handling".

SINEMA Server can send e-mails to configured recipients and execute programs as a reaction to triggered events. For SINEMA Server to send the e-mails, the e-mail settings must be configured under "Administration > System > E-mail settings"; see section Administration - System / E-mail settings (Page 214).

Basic settings

The following settings can be configured:

Parameter	Meaning
Standard e-mail recipient	E-mail addresses to which e-mails are sent if no specific e-mail recipient was configured for an event reaction. If multiple e-mail recipients are specified, these need to be separated from each other by a semi-colon (there must be no spaces).
Language	Each sent e-mail contains a system-defined, event-specific text. Here, select the language for this text.

Event reactions

In this area you can edit, enable and disable event reactions. Only enabled event reactions are triggered when the associated event occurs. You can select from the following settings in the event reactions editor:

Parameter	Meaning
Standard e-mail recipient	Display of the standard e-mail recipient configured in the basic settings
Enabled	When this check box is selected, an e-mail is sent to the configured recipient when the associated event occurs and the specified program is executed, if any.
Program	Name of a program that will be executed as a reaction to an event in the form of a process in the background. The program can be executed by SINEMA Server in the background if it is stored in a directory assigned to the system environment tag "path". Which directories are assigned to this tag is displayed after calling the "path" command in the command prompt. You can pass parameters to the program by specifying them after the program name separated by spaces. Example: program.bat 129.10.168.2 Device1 It is not possible to use dynamically filled parameters.
E-mail text	Specify a text that is to be sent by e-mail in addition to the system-defined text. In this e-mail text, the following properties of the respective device can be specified by parameters: • $i - placeholder for IP address • $m - placeholder for MAC address • $n - placeholder for device name

Parameter	Meaning
E-mail recipient	Specify the e-mail recipients that are to be informed by e-mail when the associated event occurs. The e-mail can be sent either to the standard e-mail recipient configured in the basic settings or to specific e-mail recipients. If multiple e-mail recipients are specified, these need to be separated from each other by a semicolon (there must be no spaces).
Device selection (only available for event reactions whose events can be triggered by devices)	You can specify in the device selection that the event reaction is only executed when the associated event is triggered by selected devices. The following options are available: • All devices: The event reaction is executed regardless of which devices have triggered the associated event. • Devices in view: The event reaction is only executed when the devices of the selected views have triggered the associated event. • Select devices: The event reaction is only executed when the selected devices have triggered the associated event.

4.4.4.4 Administration - Events Syslog Server

The dialog described below can be accessed via the menu command "Administration > Events > Syslog Server".

SINEMA Server can be used as a Syslog client and can send triggered events to up to 3 Syslog servers. The system events are sent to the Syslog servers in RFC 5424 format in English.

The dialog for configuring the Syslog servers in SINEMA Server is described below. The appendix to the manual describes the general structure and the meaning of the Syslog messages.

Operation

The following table explains the operator controls of the header:

Operator control	Function
	Create Syslog server Opens a dialog in which the IP address and the UDP port of the Syslog server to be created are specified and in which the Syslog server can be activated. SINEMA Server only forwards triggered events to Syslog servers that have been activated.
	Edit Syslog server Opens a dialog in which the properties of the selected Syslog server can be edited.
	Delete Syslog server Deletes the selected Syslog servers.
	Activate Syslog server Enables the selected Syslog servers. SINEMA Server only forwards triggered events to Syslog servers that have been activated.
	Disable Syslog server Disables the selected Syslog servers. SINEMA Server only forwards triggered events to Syslog servers that have been activated.

4.4.5 Administration - User

Overview

The **"Administration > User"** Web page has the following tabs:

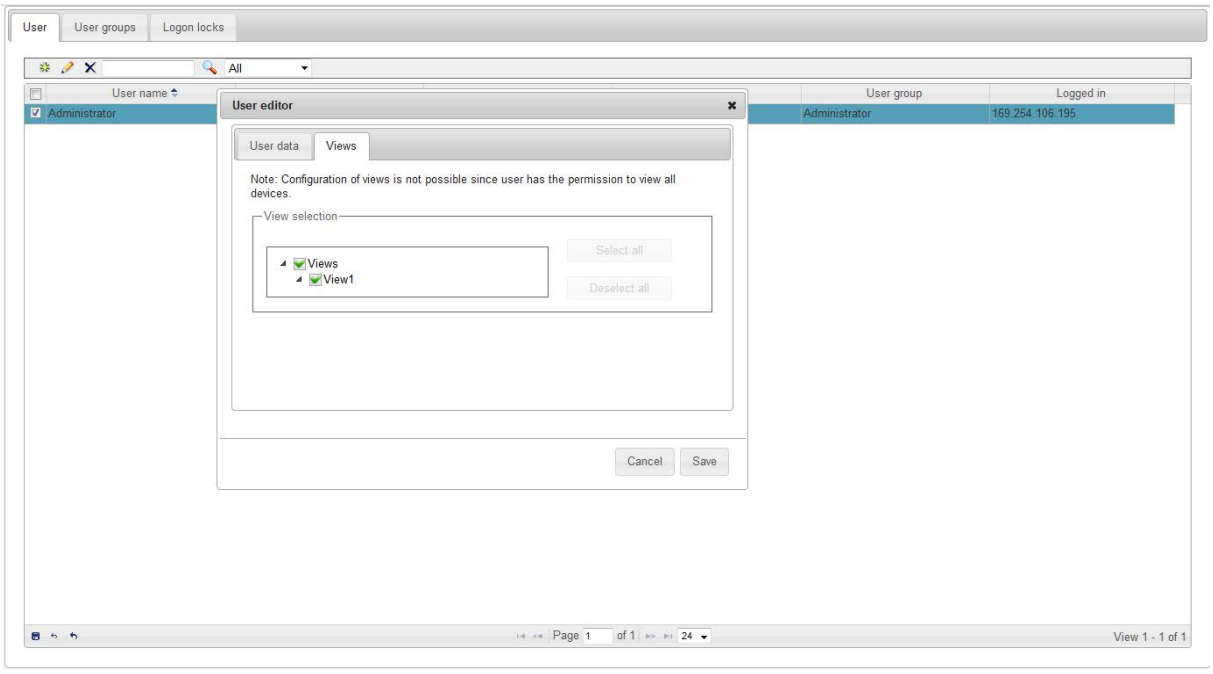
- "User"
- "Groups"
- "Logon locks"

The following explains the form, content and functionality of these tabs.

4.4.5.1 Administration - User User

You open the Web page shown below using the menu command: **"Administration > User > User"**

The figure shows the Web page with the User editor opened.



Functions

The following table explains the function elements of the header.

Icon	Display / function
	Create a new user This opens the User editor.
	Change user This opens the User editor.
	Delete user
	Enter text for text search / filter
	Start text search / enable filter The user groups containing the specified text in their names are displayed.
	Filter display: • All • Logged in • Logged off

The data area contains the user data with the following columns:

- User name
- Full user name
- E-mail
- View(s) (assigned views)

- User group
- Logged in (IP address)

If you create or change a user, another window opens with two tabs in which you can enter the user-specific data.

User editor

When you create or modify a user, a further window opens in which you can enter the user data and select the views. If the user does not have the right to "View all devices and servers", only the devices, SINEMA Server instances and validation reports that are assigned to the view of the user are displayed after the user is logged on. A PNIO system is only displayed for this user when the corresponding controller is assigned to at least one view of this user.

When entering the password for a user, the current password strength is checked. You can find the criteria for determining the password strength in the section Password strength (Page 238).

See also

Users and user groups (Page 66)

4.4.5.2 Administration - Users user groups

On the Web page “Administration > Users > User groups” you can manage user groups and activate or deactivate the rights for existing user groups in the user group editor.

Functions

The following table explains the function elements of the header.

Icon	Display / function
	Create a new user group This opens the User groups editor.
	Change user group This opens the User groups editor. Note: The "User settings" right in the "Administrator" user group cannot be disabled.
	Deleting user group
	Enter text for text search / filter
	Start text search / enable filter The user groups containing the specified text in their names are displayed.

All user groups are displayed in the data area.

User group editor

When you create or change a group, another window opens in which you can select the user rights of the respective group. These rights include:

- Server access via URL
- View reports
- Operative monitoring settings
- User settings
- Basic settings for discovery and monitoring
- View user-specific topology
- View all devices and servers
  - View all devices, SINEMA Server instances, and validation reports, regardless of their assignment to views.
  - Use topology (online mode only)
- View server overview
- System settings
- Jobs of all job types and basic job settings
- Jobs of the job type "Firmware download" and "Firmware activation" relevant basic job settings
- Jobs of the job type "CLI" and relevant basic job settings
- Job of the job type “System backup”
- Jobs of the job type "Database clean up" and relevant basic job settings
- View validation reports
  - View existing validation reports and validation report configurations
- Start and delete validation reports
  - Start and delete validation reports
  - Copy validation report configurations and create them based on validation report templates
  - Edit basic settings of validation report configurations
- Create and configure validation reports
  - Create, configure, and delete validation report configurations and templates
- Comments and events
  - Add or delete comments on devices and events
  - Resolve events manually

Procedure

In the open User Group editor, follow the steps below to create a user group and to assign one or more functions to the user group:

1. Enter a name for the new user group.
2. Select one or more entries in the table.
3. Select the "Activate" button to assign the selected functions to the user group.
4. Select the "Deactivate" button to remove the selected functions from the user group
5. Select the "Save" button to apply the settings.

4.4.5.3 Administration - User Logon locks

Protection from brute force attacks

To protect against brute force attacks, after five failed logon attempts the IP address of a user or a user the logon to SINEMA Server is rejected assuming that there was less than five minutes between the logon attempts.

Locked IP addresses / unlocking users

Locked IP addresses are displayed under "Administration > User > Logon locks" and can be unlocked by users who have the "User settings" right. Whether and after what period IP addresses or users are unlocked can be configured by users with this right using the symbol . As default, automatic unlocking is enabled.. The default and minimum value for the locking period is 10 minutes.

4.4.6 Administration - System

4.4.6.1 Administration - System System information

The **"Administration > System > System information"** Web page shows you information about the management station. This includes information about the computer, the operating system used and details of the SINEMA Server installation.

4.4.6.2 Administration - System configuration

Meaning

In this dialog, you can export your system configuration, import an exported system configuration and reset your system configuration to initial values.

In this dialog, you also specify the shared secret for access to data of other SINEMA Server instances. Before a SINEMA Server instance can query device data of another SINEMA

Server instance and display it in the server overview, the same shared secret must be configured for both of them.

With the **"Administration > System > Configuration"** menu command, you obtain the following buttons and functions:

"System configuration" dialog area:

- "Export" button

  To export the system configuration, click the "Export" button. The following settings can be saved on a specified path:

  – Scan settings
  – Device profiles
  – General monitoring settings
  – PROFINET diagnostics text library
  – Event types / event reactions / overall status groups
  – "Unmanaged" device types
  – Users and user groups
  – Filter templates
  – Validation report templates
  – Basic settings of the basic job settings
  – Settings of the job type "Firmware download" of the basic job settings
  – Settings of the job type "CLI" of the basic job settings
  – System job types

  If you want to change the proposed file name for the export file, you need to specify the file extension .ENC manually. Otherwise the export file will be saved in the wrong format

  Before exchanging system configurations, refer to the recommendations in the section Central configuration of device profile data (Page 40). When exporting job-relevant settings, also note the special points in the section Basic settings (Page 232).

- "Import" button

  To import an existing system configuration, click on the "Import" button and select the file to be imported in the pop-up dialog using the "Browse" button.

  Importing a system configuration is only possible when there are currently no devices in the system.

  Before exchanging system configurations, refer to the recommendations in the section Central configuration of device profile data (Page 40). When importing job-relevant settings, also note the special points in the section Basic settings (Page 232).

- "Reset" button

  To reset certain settings of the system configuration, click the "Reset" button. A dialog box with options opens in which you can make your selection.

  Resetting a system configuration is only possible when there are currently no devices in the system.

"Server overview" dialog area: Entry of the shared secret. When the shared secret is entered, the current password strength is checked. You can find the criteria for determining the password strength in the section Password strength (Page 238).

4.4.6.3 Administration - System / E-mail settings

Before you can configure an event reaction in "Administration > Events > Event reaction", you need to configure e-mail settings for the sender of e-mails under "Administration > System > E-mail settings". These e-mails are sent as reaction to the events that have occurred. The following needs to be specified:

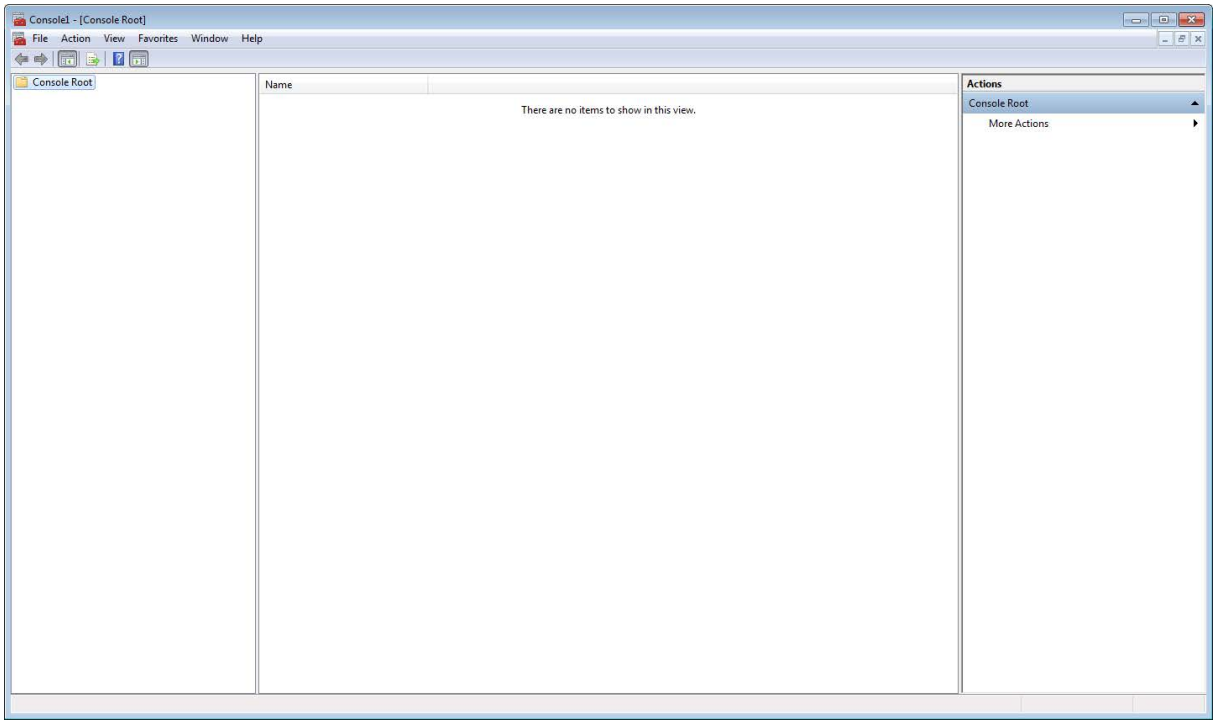
- SMTP server IP
- SMTP port
- Email address of the sender
- User name (optional)
- Password / password confirmation (optional)
- Encryption (selection from drop-down list)

When the password is entered, the current password strength is checked. You can find the criteria for determining the password strength in the section Password strength (Page 238).

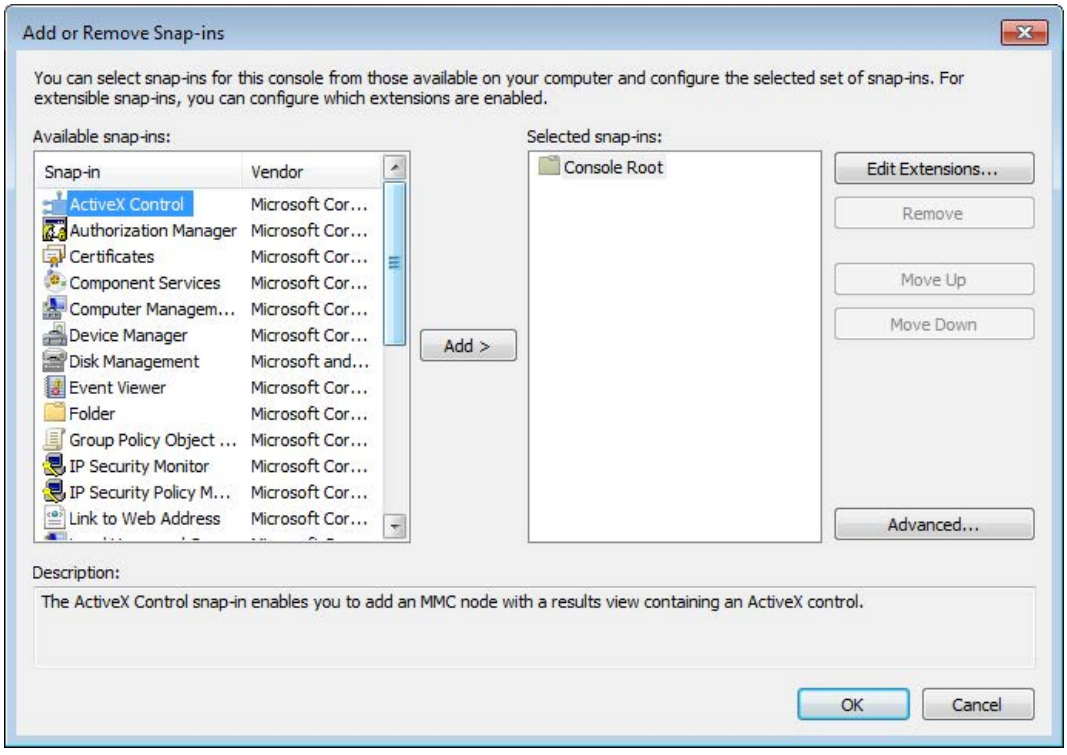
Importing a certificate into the certificate store

When using SSL or TLS for encryption, the certificate of the mail server must be imported into the certificate store of the management station if the certificate does not exist in this certificate store or if it is a self-signed certificate. Follow the steps outlined below:

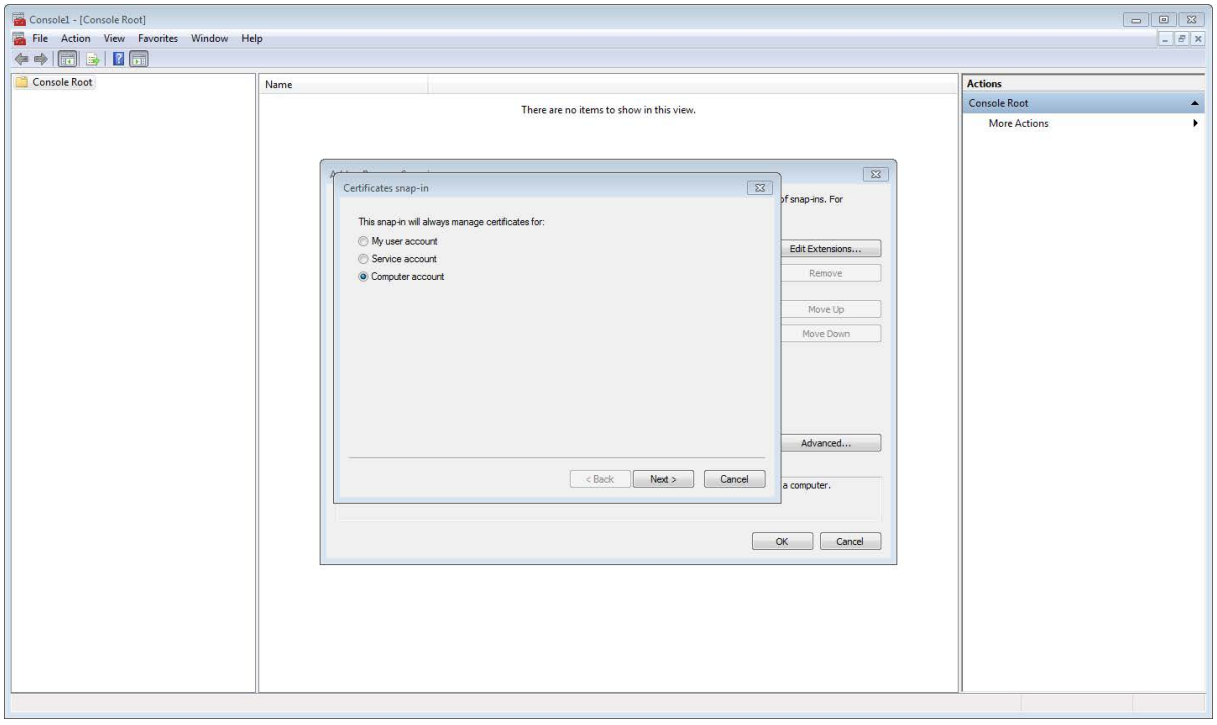
1. Call the Microsoft Management Console in the command prompt of the management station with the character string "mmc".



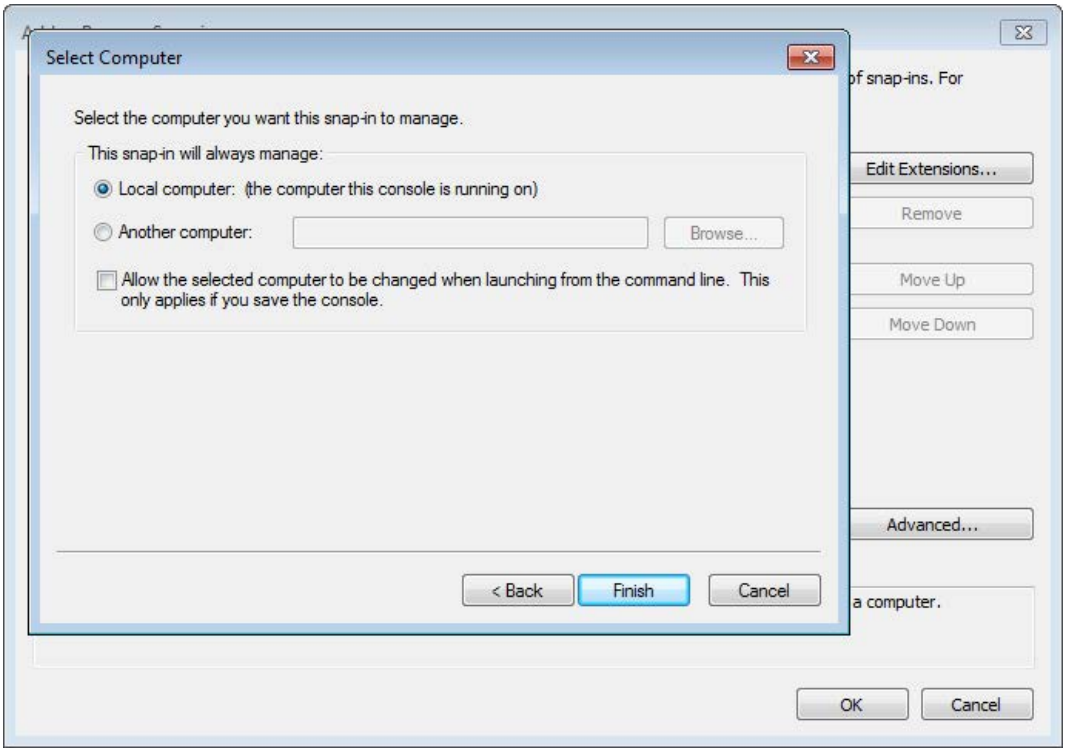
2. Select the menu command "File" > "Add/Remove Snap-in...".
3. From the "Available snap-ins" list, select the entry "Certificates" and click the "Add" button.



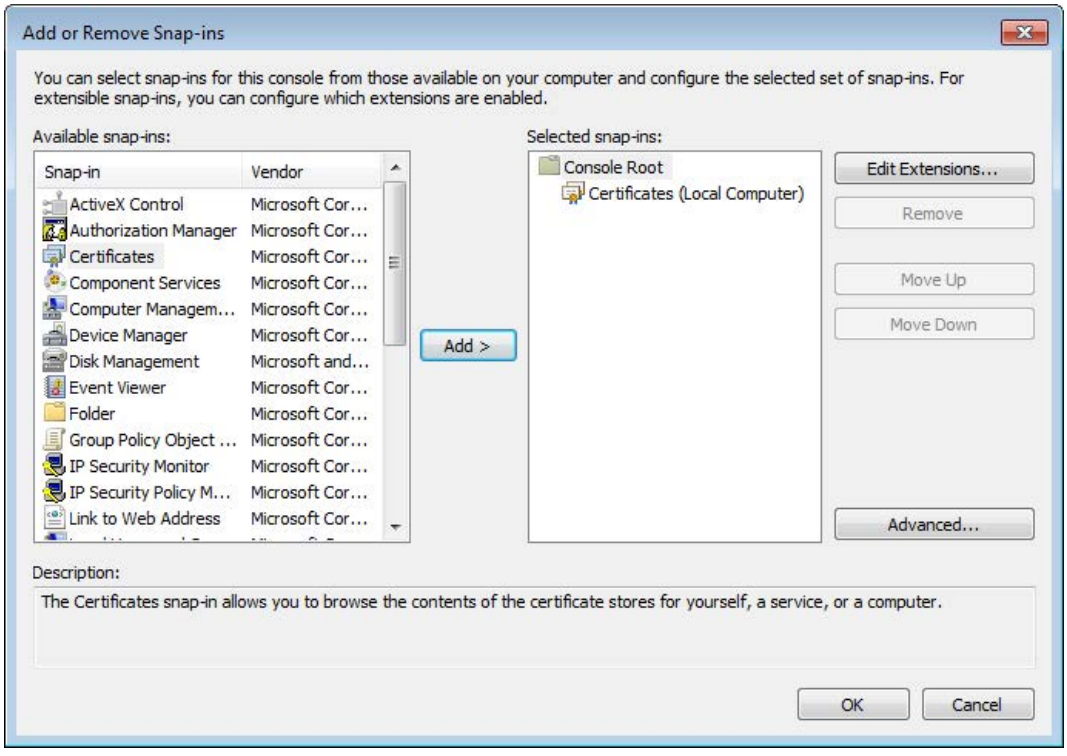
4. Select the "Computer account" option and click the "Next" button.



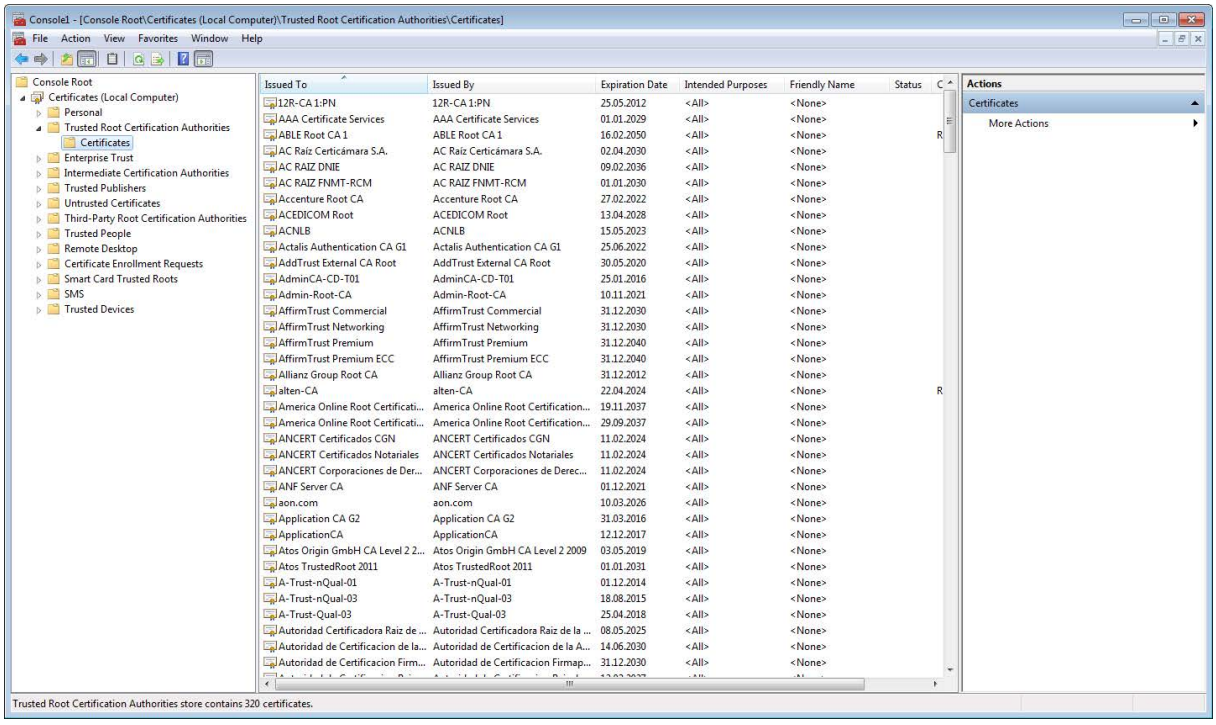
5. Make sure that in the setting "This snap-in will always manage" the option "Local computer" is selected and click the "Finish" button. The certificate store of the local computer is now shown in the list of selected snap-ins.



6. Click the "OK" button.



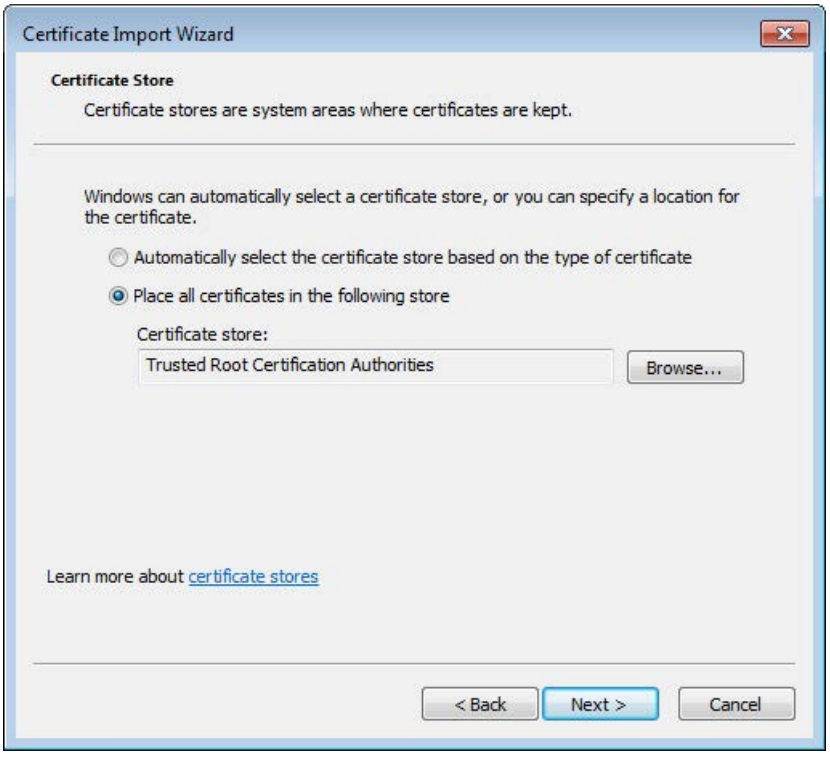
7. In the folder structure on the left-hand side, navigate to the "Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates" folder.



8. In the shortcut menu of the "Certificates" folder, select the menu command "All Tasks > Import...".
9. Click the "Next" button.

10. With the "Browse" button select the certificate of the mail server and click the "Next" button.

11. Make sure that in the following window the option "Place all certificates in the following store" and the certificate store "Trusted Root Certification Authorities" are selected.



12. Click the "Next" button and then the "Finish" button.
13. Close the Microsoft Management Console, exit SINEMA Server and restart the PC.

4.4.7 Administration - My settings

4.4.7.1 Administration - My settings Password

The window contains the usual fields for changing a password:

- Previous password
- New password
- Confirm new password

The current password strength is checked during input. You can find the criteria for determining the password strength in the section Password strength (Page 238).

4.4.7.2 Administration - My settings User interface

The **"Administration > My settings > User interface"** Web page includes the "Monitoring refresh interval" box. With the monitoring interval, you specify the number of seconds after which the data in the user interface is updated. This can be adjusted between 10 and 120 seconds and the minimum value is 15 seconds.

You can save the value using the icon in the header.

4.4.8 Administration - Jobs

4.4.8.1 Overview

Function of jobs

A job is a set of tasks that can be executed in SINEMA Server. When a job is executed for devices every device is process in a task of this job. A maximum of 100 tasks can be processed in one job.

Jobs can be created, plan and started manually or time-controlled in SINEMA Server. While jobs are executing, simultaneous use of other functions of SINEMA Server is possible. The processing status of jobs and the corresponding tasks can be viewed at any time and are also communicated by the corresponding events

Available job types

The following types of job are available in SINEMA Server:

- Run a firmware download (and optional activation) for SCALANCE X and SCALANCE W devices
- Firmware activation for SCALANCE X and SCALANCE W devices by restarting the devices
- Execute CLI commands
- Create system backup
- Run database cleanup

Note

Jobs of the job type "System backup" and "Database cleanup"

A job of the type "System backup" must not be executed while a job of the job type "Database clean up" is executing. The reverse also applies. Between the end of job execution of the job type "Database cleanup" and the start of job execution of the job type "System backup" there must be at least a 10 minute gap. These restrictions apply both to manual and planned job executions.

See also

Basic job settings (Page 231)

Configuration of jobs (Page 225)

4.4.8.2 Requirements for the execution of jobs

Before jobs can be executed, the following job type-specific requirements must be met.

Job type "Firmware download"

Before jobs of the type "Firmware download" can be executed, the following requirements must be met:

- TFTP server:

  A TFTP server is required that can be reached from the management station and from the devices and on which the firmware files can be stored. When there is a firmware download, the devices then obtain the firmware files from this TFTP server. The TFTP server is not part of the SINEMA Server product package.

  You configure the TFTP server in SINEMA Server in the "Firmware download" tab of the basic job settings.

  The TFTP server used should be protected by a firewall.

- Firmware files

  The firmware files need to be stored in the firmware storage of SINEMA Server via the basic job settings. Files stored there are copied automatically by SINEMA Server to the basic directory specified for the TFTP server. You specify which firmware files can potentially be used for a device by adding a firmware file to the firmware storage and specifying the article numbers for which the firmware file will be valid. When configuring a job, only the firmware files valid for devices are available.

- Hardware Support Packages (HSPs):

  HSPs contain instructions required by SINEMA Server among other things for running firmware downloads to devices. For every device for which a firmware download will be performed an HSP identified with the article number of this device is required. HSPs for the supported Siemens devices already exist in SINEMA Server and are named with the article numbers of the corresponding devices. Whether the HSPs required for a firmware download for the article numbers assigned to a firmware file exist is shown in the “HSP support" column: “Firmware download" is shown in the "Firmware download” tab of the basic job settings. If several HSPs for at least one of the assigned article numbers, the entry "Yes" is highlighted in red in the table column. In this case, check the HSP assignment because SINEMA Server itself selects one of the HSPs in this case. In the "Basic settings” tab of the basic job settings new HSPs can be added and the list of HSPs already added to article numbers can be edited.

Job type “Firmware activation”

For every device whose firmware will be activated an HSP identified with the article number of this device is required. HSPs for the supported Siemens devices already exist in SINEMA Server and are named with the article numbers of the corresponding devices. Whether the HSPs required for a firmware activation for the article numbers assigned to a firmware file exist is shown in the “HSP support" column: “Firmware activation" is shown in the "Firmware download” tab of the basic job settings. If several HSPs for at least one of the assigned article numbers, the entry "Yes" is highlighted in red in the table column. In this case, check the HSP assignment because SINEMA Server itself selects one of the HSPs in this case. In the "Basic settings” tab of the basic job settings new HSPs can be added and the list of HSPs already added to article numbers can be edited.

Job type "CLI"

Before jobs of the type "CLI" can be executed, the following requirements must be met:

- CLI scripts:

  The CLI scripts need to be stored in the CLI script storage of SINEMA Server via the basic job settings. You specify which CLI scripts can potentially be used for a device by adding a CLI script to the CLI script storage, selecting the compatibility type "Restricted" and then specifying the article numbers of the devices for which the CLI script will be valid. When you configure a job, after selecting this CLI script, only the devices valid for it are available for selection. If you have selected the combat ability type "Universal", all monitored devices are available for selection in the device assignment.

- Hardware Support Packages (HSPs):

  For every device for which a CLI script will be executed an HSP identified with the article number of this device is required. HSPs for the supported Siemens devices already exist in SINEMA Server and are named with the article numbers of the corresponding devices.

Job type “System backup”

A job already exists for the job type "System backup" that executes as default every day at 04.00 am. To execute this job and HSP is required that already exists in SINEMA Server.

A created system backup can be transferred back manually via SINEMA Server Monitor. If SINEMA Server cannot be started correctly, the last created system backup is transferred back automatically. The path on which SINEMA Server searches for this system backup can be configured in the job type-specific settings, refer to the section Job type-specific settings for the job type "System backup" (Page 229).

Job type "Database cleanup"

For the job type "Database cleanup" there is already a job with the type of execution "Manual". To execute this job an HSP is required that already exists in SINEMA Server.

The basic job settings are described in section Basic job settings (Page 231).

This configuration of jobs is described in sectionConfiguration of jobs (Page 225).

Layout of the Web page

The Web page “Administration > Jobs" displays all the jobs stored in SINEMA Server with their configured properties and status information.

With the control elements of the header, jobs can be managed and controlled for execution.

Operator input

The following table explains the control elements of the header.

Symbol	Function
	Add new jobr The dialog for configuring jobs is displayed, see section Configuration of jobs (Page 225).
	Copy selected job The selected job is copied and the configuration dialog for the new job is opened. The settings of the copied job are adopted including the devices assigned to the job and can be adapted. Copying makes sense, for example when creating a job to activate a firmware file based on a job for downloading a firmware file, when both jobs will be executed for the same devices. This function is not available for the job type "System backup".
	Edit selected job The dialog for configuring jobs is opened, see section Configuration of jobs (Page 225).
	Delete selected jobs The selected job is deleted. Multiple selection is possible. Jobs in the “In progress” status cannot be deleted. This function is not available for the job type "System backup".
	Basic job settings The dialog for configuring the basic job settings is opened, see section Basic job settings (Page 231).
	Run selected jobs The selected job is started from the beginning and changed to the "In progress" status. Multiple selection is possible. The execution started with this but has no influence on executions planned for the job.
	Pause / suspend selected jobs The function of this button depends on the status of the selected job: • Job status “In progress”: The selected job is paused and changed to the “Paused" status. Tasks of the job currently being processed are executed where possible to the end. However no new tasks are started. This function is not available for the job types "System backup" and "Database clean up". • Job statuses “Pending / Finished / Stopped / Failed partly / Failed”: Jobs in one of these statuses and not configured with the type of execution "Manual" are changed to the "Suspended" status. For jobs in the "Suspended" status, planned executions are not performed and changes to their configuration are not possible. This button has no influence on jobs in other statuses.

Symbol	Function
	Continue selected jobs / cancel suspension of jobs The function of this button depends on the status of the selected job: • Job status "Paused": The selected job is continued from the position at which the job was paused. • Job status "Suspended": The selected job is changed to the "Pending" status and executed again according to the planning configured for it. This button has no influence on jobs in other statuses.
	Stop selected jobs A job in the status "In progress" is stopped with this button and cannot be continued at the same position If the type of execution "Manual" was configured for the job, it is given the status "Stopped". Tasks of the job currently being processed are executed where possible to the end. However no new tasks are started. Multiple selection is possible.
	Stop / suspend all jobs The function of this button depends on the status of the job: • Job status “In progress”: Refer to the description of the "Stop selected jobs” function. • Job status “Pending / Finished / Stopped / Failed partly / Failed”: Jobs in one of these statuses and not configured with the type of execution "Manual" are changed to the "Suspended" status. For jobs in the "Suspended" status, planned executions are not performed and changes to their configuration are not possible. Regardless of the jobs involved, the buttons "Run selected jobs”, “Pause / suspend selected jobs” and “Stop selected jobs” are disabled. By clicking the "Stop / suspend all jobs" button again the buttons are re-enabled and planned executions of jobs are performed again.
	Enter text to filter based on jobs. The entered text is searched for in all columns. In the input box, text is displayed when a simple query entered in the filter template editor is active. The {} icon is displayed when a filter template with a complex query is active.
	Selection of a previously created template for filtering according to jobs. After selection, the properties of the filter template are applied to the list of jobs. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
	Open the editor for configuring filter settings that can be stored in filter templates. The icon is displayed when the configured filter settings differ from the default filter settings.

Task statuses

The "Task" column displays the total number of tasks of a job. Behind the total number, it is displayed how many tasks have which status. The statuses are indicated by colors:

Color	Task status
Green	Task was executed successfully.
Red	An error occurred when executing the task
Gray	Task status is unknown

4.4.8.3 Configuration of jobs

Overview

You reach the dialog for configuring jobs via the button for creating, editing or copying a job or using the shortcut menu command "Advanced settings > Add new job" in the device list. In this dialog you can make basic settings not dependent on the job type and job type-specific settings and assign the required devices to a job. After using the shortcut menu command, the selected devices are already assigned to the job. The settings cannot be changed for jobs that are currently being executed.

Basic settings

The "Basic settings" tab contains the following parameters:

Parameter	Function
ID	ID of the job that is generated automatically when the job is saved. The ID cannot be changed.
Status	Current status of the job. A job as the status "Draft" until all the properties required to execute it are configured. Afterwards the job is set to the "Pending" status and can be executed. For information on other job statuses, refer to the section Requirements for the execution of jobs (Page 221)
Description	Freely selectable description of the job.
Tasks	Display of the total number of tasks contained in the job. Behind, the statuses of the tasks during the last job execution are shown, see section Requirements for the execution of jobs (Page 221).

Parameter	Function
Type of execution	With this drop-down list, the type of execution of the job can be specified: • Manual: The job can only be executed using the buttons "Run selected jobs" in the header of the job list and "Save and execute" in the configuration dialog for jobs. • Once: The job is executed once at a selectable time. The job can also be executed with the "Run selected jobs" button. • Every n hours: As of a selectable point in time the job is executed at a selectable interval of hours. The minimum value is 1, the maximum value 24. The end of the periodic execution can be specified with a number of executions or with end date. The job can also be executed using the "Run selected jobs" button. The "Every n hours" option is not available for the job type "Database cleanup". • Every n days: As of a selectable point in time the job is executed at a selectable interval. As the interval, the options "Daily", "Weekly", "Monthly" or a user-defined number of days can be selected. The end of the periodic execution can be specified with a number of executions or with end date. The job can also be executed using the "Run selected jobs" button. The "Every n days" option is not available for the job type "Database cleanup". • Every n months: As of a selectable point in time the job is executed at a selectable interval. As the interval, the options "Monthly", "Yearly" or a user-defined number of months can be selected. The end of the periodic execution can be specified with a number of executions or with end date. The job can also be executed using the "Run selected jobs" button. The "Every n months" option is only available for the job type "Database cleanup". For jobs configured with a type of execution other than "Manual", no logon to SINEMA Server is necessary.
Job type	With the job type, you specify the function of the job: • Firmware download: Runs a firmware download for SCALANCE X and SCALANCE W devices. As an option, the firmware can be activated after the update. • Firmware activation: Activates the firmware of a SCALANCE X or SCALANCE W device by restarting the device. • CLI: Executes a CLI script. • System backup A system backup contains all the project and program data including the monitored devices and events. This job type is selected already as default for an existing job. The job type for this job cannot be changed and no further jobs with this job type can be configured. • Database cleanup: Cleans up archive data foe reports and events in the SINEMA Server database. Prior to deletion, the archive data can be exported for reports. It is also possible to import this archive data. The effects of a database cleanup take effect only after restarting SINEMA Server. A maximum of 11 jobs of this job type can be created.

Job type-specific settings for the job type "Firmware download"

For the job type "Firmware download" the "Job type specific settings" tab contains the following parameters:

Parameter	Function
Maximum number of tasks performed at the same time	Specifies the maximum number of tasks of the job that can be performed at one time. Each device is processed in its own task. The minimum value is 1, the maximum value of the cross-job value configured in the basic job settings..
Run firmware activation	As the mode of firmware activation, one of the following options can be selected: • After the firmware downloads for all devices have been made • Immediately after the firmware download to a device • Do not execute
Use following firmware	With the following options you specify which firmware file will be used when downloading to the devices assigned to the job. A device-specific selection in the "Devices" tab overwrites the selection in this tab. • Default firmware: For a device the firmware file is used for which the article number of the device is specified in the basic job settings and that is configured there as default firmware. If several firmware files are configured as the default firmware for the article number, the firmware file with the highest identified firmware version is used. • Newest firmware For a device the firmware file is used for which the article number of the device is specified in the basic job settings. If several firmware files come into question, the firmware file with the highest identified firmware version is used. This is shown in the "Firmware download" tab of the basic job settings.
If an error occurs:	With the following options you specify is how a failed task execution is handled: • Continue with following tasks Execution continues with the following tasks of the job. • Do not run following tasks: All the following tasks of the job are no longer run. Tasks already being run continue to be executed.
Configuration backup	If this check box is enabled, prior to running firmware downloads to the devices of the job, their configurations are saved automatically on the TFTP server. A configuration file has the file extension *.cfg and is named with the IP address of the device and the time stamp of the creation of the file. It is not possible to restore configuration files using SINEMA Server. The creation of automatic configuration backups by SINEMA Server is particularly useful before performing firmware downgrades since here the device configurations can be lost.

Job type-specific settings for the job type "Firmware activation"

For the job type "Firmware activation" the "Job type specific settings" tab contains the following parameters:

Parameter	Function
Maximum number of tasks performed at the same time	Specifies the maximum number of tasks of the job that can be performed at one time. Each device is processed in its own task. The minimum value is 1, the maximum value of the cross-job value configured in the basic job settings..
If an error occurs:	With the following options you specify is how a failed task execution is handled: • Continue with following tasks Execution continues with the following tasks of the job. • Do not run following tasks: All the following tasks of the job are no longer run. Tasks already being run continue to be executed.

Job type-specific settings for the job type "CLI"

For the job type "CLI" the "Job type specific settings" tab contains the following parameters and control elements:

Parameter / control element	Function
Script name	Display of the name of the CLI script that was selected with the "Select" button.
Select	Opens a dialog in which a CLI script can be selected that was saved in the CLI script storage via the basic job settings: If the job has already been assigned devices, this dialog displays the CLI scripts valid for these devices and CLI scripts with the type of validity "Universal".
Description	Display of the description of the CLI script that was selected with the "Select" button.
Details	Opens a dialog that displays the settings, CLI commands and article numbers of the CLI script. No changes can be made in this dialog.
User name	Specifies the user name required for execution of the CLI scripts for the devices assigned to the job. Only one user name can be specified for each job. Specifying a user name is optional, the maximum number of characters is 25.
Password	Specifies the password of the selected user. The maximum number of characters is 25. When the password is entered, the current password strength is checked. You can find the criteria for determining the password strength in the section Password strength (Page 238).
SSH port (encrypted)	The "SSH" protocol and the specified port are used for communication with the devices for which the CLI scripts will be run. The setting made here overwrites settings from the basic job settings. For security reasons the "SSH" protocol should be used for communication with the devices.
Telnet port (unencrypted)	The "Telnet" protocol and the specified port are used for communication with the devices for which the CLI scripts will be run. The setting made here overwrites settings from the basic job settings.
Use basic job setting	The protocol and the port that was selected in the basic job settings are used for communication with the devices.

Parameter / control element	Function
Maximum number of tasks performed at the same time	Specifies the maximum number of tasks of the job that can be performed at one time. Each device is processed in its own task. The minimum value is 1, the maximum value of the cross-job value configured in the basic job settings..
If an error occurs:	With the following options you specify is how a failed task execution is handled: • Continue with following tasks Execution continues with the following tasks of the job. • Do not run following tasks: All the following tasks of the job are no longer run. Tasks already being run continue to be executed.

Job type-specific settings for the job type "System backup"

For the job type "System backup" the "Job type specific settings" tab contains the following parameters:

Parameter	Function
Number of system backups	Number of system backups stored on the configured path on the management station. If the specified number is reached, the next system backup automatically deletes the system backup with the oldest time stamp. The minimum value is 1, the maximum value 10.
Path for system backups on management station	Pass on the management station on which system backups are saved and on which SINEMA Server searches for the last created system backup when automatically restoring. Paths to network drives are not permitted.

Job type-specific settings for the job type "Database cleanup"

For the job type "Database cleanup" the "Job type specific settings" tab contains the following parameters:

Parameter	Function
Entries to be deleted	If you have selected the type of execution "Manual" or "Single", the following options are available: • Entries older than Entries before the specified month and year are deleted. The specified month must be before the current month. • Entries for events between Entries between the specified start and end date are deleted. With this option, only event-relevant archive data can be deleted. If you have selected the type of execution "Every n months", you can specify a number of months. Entries that are older are deleted. Permitted range of values: 1 ... 120 months.
Event categories / event classes	Selection of event categories and event classes whose events will be deleted. Events in the status "Pending" cannot be deleted.
Report archives	• None: No action is taken. • Delete archives: Archive data relevant for reports is deleted • Delete archives of deleted devices: Archive data relevant for reports of all deleted devices is deleted regardless of the specified time frame for entries to be deleted. • Export archives and delete: Archive data relevant for reports is exported to a specified directory on the management station and then deleted in SINEMA Server. It is not possible to export to network drives. • Import archives - path on management station (only for the types of execution "Manual" and "Single"): Archive data relevant for reports is imported from the specified directory on the management station. If no path is specified, there is no import. Importing from network drives is not possible. ZIP files generated by SINEMA Server should not be edited prior to import. It is not possible to import edited ZIP files.

Device settings

Overview

In the "Devices" tab, you can assign the required devices to the job using the horizontal arrow buttons. Only monitored devices can be assigned. In addition to this, the selection of the assignable devices can be restricted depending on the selected job type. When the job was created in the device list using the shortcut menu "Advanced settings > Add new job", the selected devices are already assigned to the job.

The order of the assigned devices to be processed can be specified using the vertical arrow buttons in the header. If the simultaneous processing of several tasks is permitted, the configured processing order can differ from the real order.

For jobs whose execution has already started, only the area of the assigned devices is displayed. In this view, the task status is displayed in the "Status" column. For failed tasks, the cause of the error is shown in a tooltip.

For the devices the IP addresses are shown via which SINEMA Server can reach the devices. In the case of NAT devices these are the external IP addresses on the NAT router.

Below the job type-specific properties of the assignment dialog are described.

Device settings for the job type "Firmware download"

If a job of the type "Firmware download" is involved, in the area of the assigned devices, you can call up a dialog for selecting a firmware file for each device using the button. Multiple selection is only possible for devices that have the same article number. In the dialog, all the firmware files located in the firmware storage of SINEMA Server are displayed that are identified with article number of the selected device. The selection in this dialog overwrites the configuration made in the job type-specific settings. Based on the examples of entries, the following table explains how the selection dialog works:

Entry	Effect on selection
V2.0	The firmware file with the name V2.0 is always used.
Default firmware (V2.5)	For a device the firmware file is always used for which the article number of the device is specified in the basic job settings and that is configured there as default firmware. In the firmware files that are configured as the default firmware for the article number, the firmware file with the highest identified firmware version is used. Currently this is version V2.5.
Newest firmware (V3.0)	The firmware file with the highest identified firmware version of the firmware files valid for the article number of the device is always used. Currently this is version V3.0.

In the area of the assigned devices, the “Current firmware version" column shows the firmware currently on the device and the "Firmware download" column shows the configured firmware download behavior. If a concrete firmware version was selected in the selection dialog described above, the text “User-defined" is displayed in this column. Otherwise the option selected in the job type-specific settings is displayed.

Device settings for the job type "Firmware activation"

In the area of the assigned devices, the “Current firmware version" column shows the firmware currently on the device. The firmware cannot be changed for the assigned devices.

Device settings for the job type "CLI"

If a CLI script with the compatibility type "Universal" was selected in the job type-specific settings, all monitored devices are available for selection in the "Available devices" area. If the combat ability type "Restricted was selected only the monitored devices valid for the CLI script are available for selection.

For jobs that have already been executed, the symbol can be used to display the course of execution of the CLI script.

4.4.8.4 Basic job settings

Overview

In the basic job settings, you can make cross-job type and job type-specific settings. It is also possible to export and import basic job settings you have made. The "Events” tab shows all the job-relevant events that have occurred. These are also displayed in the event list.

Basic settings

In the basic settings, the following parameters and control elements are available:

Parameter / control element	Function
Maximum number of tasks performed at the same time	Specifies the maximum number of tasks that can be performed at one time. The specified number applies to the tasks of jobs of all job types. The minimum value is 1, the maximum value 25.
Export	Opens a dialog in which the parts of the basic job settings to be exported can be selected. The export of basic job settings is not possible during the execution of jobs. For this reason, SINEMA Server automatically runs the function “Stop / suspend all jobs” after clicking the “Export” button. After the export has been performed, planned executions of jobs are performed again. It is not possible the change the basic job settings during export. If you want to change the proposed file name for the export file, you need to specify the file extension .ENC manually. Otherwise the export file will be saved in the wrong format
Import	Opens a dialog in which the parts of the basic job settings to be imported can be selected. Due to importing, the selected parts of the basic job settings are completely overwritten. Tasks whose firmware files are overwritten by the import can therefore fail. The import of basic job settings is not possible during the execution of jobs. For this reason, SINEMA Server automatically runs the function “Stop / suspend all jobs” after clicking the “Import” button. After the import has been performed, planned executions of jobs are performed again. It is not possible the change the basic job settings during import.
	Add new HSP Opens a dialog in which a Hardware Support Package (HSP) can be selected for import.
	Edit selected HSP Opens a dialog in which a descriptive text for the HSP and a waiting time for a response from devices can be specified in seconds. In addition to this, article numbers of devices for which the HSP is valid can be specified, changed and deleted. Only HSPs for the job types “Firmware download” and “Firmware activation” can be edited.
	Delete selected HSPs Deletes the selected HSP. Multiple selection is possible. Tasks that use a deleted HSP fail.
	Searches the list of HSPs for the entered text.

See also

Requirements for the execution of jobs (Page 221)

Firmware download

The following parameters and control elements are available:

Parameter / control element	Function
TFTP server	IP address of the TFTP server The TFTP server must be reachable from the management station and from the devices.
Port	The port used for the connection to the TFTP server. The default port is 69.

Parameter / control element	Function
Number of retries	Number of attempts to perform a firmware download after a firmware download failed. The minimum and default value is 1, the maximum value 3.
Time between retries	Time in seconds between the retries. The minimum and default value is 30 seconds, the maximum value 180 seconds.
	Add new firmware file Opens a dialog for selecting a firmware file. After the selection, an editor is opened for the firmware file, see table “Editor for firmware files” below. The maximum permitted file size for firmware files is 100 MB.
	Copy article numbers and add new firmware file Copies the article numbers of the selected firmware file and adds these article numbers to a firmware file that can be added by SINEMA Server in a dialog for firmware storage If the firmware file selected in the basic job settings is a file with the extension .SFW, the two following copying options are available: • Ignore article numbers of the new firmware file The article numbers of the firmware file selected in the basic job settings are added to the new firmware file. Existing article numbers of the new firmware file are deleted • Merge article numbers of both firmware files: The article numbers of the firmware file selected in the basic job settings are added to the new firmware file. Existing article numbers of the new firmware file are retained. Any duplicates are removed. If the firmware file selected in the basic job settings is a file with another extension, the article numbers of the new firmware file are ignored.
	Edit selected firmware file Opens the editor for editing the selected firmware file that is described in the table “Editor for firmware files”.
	Delete selected firmware files Deletes the selected firmware files from the firmware storage of SINEMA Server. The firmware file on the TFTP server is not deleted. Tasks with the deleted firmware file fail.
	Mark as default firmware Marks the selected firmware files as default firmware for the corresponding article numbers. If several firmware files are configured as default firmware for an article number, SINEMA Server uses the firmware file with the highest identified firmware version as default firmware. So that the firmware file is used for a device with one of these article numbers, “Default firmware” must be selected in the job type-specific settings for the job, see section Job type-specific settings for the job type "Firmware download" (Page 227).
	Remove designation as default firmware Removes the designation as default firmware from the selected firmware files.
	Copy selected firmware files to TFTP server Deletes the selected firmware files from the firmware storage of SINEMA Server to the basic directory configured for the TFTP server.
	Enter text to filter based on firmware files. The entered text is searched for in all columns. In the input box, text is displayed when a simple query entered in the filter template editor is active. The {} icon is displayed when a filter template with a complex query is active.

Parameter / control element	Function
	Selection of a previously created template for filtering according to firmware files. After selection, the properties of the filter template are applied to the list of firmware files. Unsaved filter settings are indicated by the "*" character. As an alternative to selecting from the drop-down list, you can also enter the name of the filter template. Cross-user filter templates are displayed in a blue font.
	Open the editor for configuring filter settings that can be stored in filter templates. The  icon is displayed when the configured filter settings differ from the default filter settings.

Table 4- 27 Editor for firmware files

Parameter / control element	Function
Firmware version	Firmware version that was read by SINEMA Server from the selected firmware file. The read out firmware version can be changed manually and is used to form the identified firmware version. The specified firmware version must contain a valid combination of periods and digits.
Description	Freely selectable description of the firmware file.
Default firmware	Marks the firmware file as default firmware for the corresponding article numbers. If several firmware files are configured as default firmware for an article number, SINEMA Server uses the firmware file with the highest identified firmware version as default firmware. So that the firmware file is used for a device with one of these article numbers, “Default firmware” must be selected in the job type-specific settings for the job, see section Job type-specific settings for the job type "Firmware download" (Page 227).
Identified firmware version	The firmware version identified by SINEMA Server from the “Firmware version” parameter. The identified firmware version is used among other things to identify the firmware file to be used for a device when several firmware files come into question for the device. In this case, the firmware file with the higher identified firmware version is used.
	Add new article number Opens a dialog in which the article numbers of devices can be specified for which the firmware file is valid. The article numbers read out of the firmware file by SINEMA Server are displayed in the table “Compatible article numbers”. It is recommended that you check whether the article numbers read out are actually compatible with the firmware file.
	Edit selected article number Opens a dialog for editing the article numbers.
	Delete selected article numbers Deletes the selected article numbers for the firmware file.
	Searches the list of article numbers for the entered text.

CLI

The following parameters and control elements are available:

Table 4- 28 Basic settings

Parameter / control element	Function
Number of retries	Number of attempts to execute a CLI script, after a device has not responded to the execution of the script. After a response from the device is missing, the entire CLI script is executed again. The minimum and default value is 1, the maximum value 3.
Time between retries	Time in seconds between the retries. The minimum and default value is 30, the maximum value 300.

Table 4- 29 Communication

Parameter / control element	Function
SSH port (encrypted)	The "SSH" protocol and the specified port are used for communication with the devices for which CLI scripts will be run.
Telnet port (unencrypted)	The "Telnet" protocol and the specified port are used for communication with the devices for which CLI scripts will be run.

Table 4- 30 Keywors for failed execution

Parameter / control element	Function
	Add new keyword Opens an editor in which a keyword and corresponding description can be specified. If the specified keyword fully matches one or more consecutive words of the execution sequence the corresponding task receives the status "Failed". By default, the CLI script does not fail if the specified keyword only matches part of a character string of the execution sequence. To achieve this, the check box in the settings for keywords must be enabled, see below. Upper and lower case characters are not taken into account when the keywords are checked. Example with the check box disabled (default setting): Execution sequence "Wrong command:" CLI script does not fail with the keyword "Wrong command". Permitted character length for keywords: 4 to 30 characters Maximum number of keywords: 10 keywords
	Edit selected keyword Opens the editor for editing the keyword and the associated description.
	Delete selected keywords Deletes the selected keywords.

Parameter / control element	Function
	Settings for keywords When you select the check box in this dialog, CLI scripts also fail when a keyword only matches part of a character string of the execution sequence. Example with the check box enabled: Execution sequence "Wrong command:" CLI script also fails with the keyword "Wrong command".
	Searches the list of keywords for the entered text.

Table 4- 31 CLI scripts and compatible article numbers

Parameter / control element	Function
	Add new CLI script Opens an editor in which the settings and commands of the CLI script can be stored. The editor is described in the table "Editor for CLI scripts". A maximum of 1000 scripts can be stored in the CLI script storage of SINEMA Server.
	Edit selected CLI script Opens the editor for editing the settings and the commands of the selected CLI script. The editor is described in the table "Editor for CLI scripts".
	Delete selected CLI scripts Deletes the selected CLI script from the CLI script storage of SINEMA Server. Tasks with the deleted CLI script fail.
	Copy selected CLI script The selected CLI script is copied and the editor for the new CLI script is opened in which settings and commands can be changed.
	Searches the list of CLI scripts for the entered text.

Table 4- 32 Editor CLI scripts

Parameter / control element	Function
Name	Freely selectable name for the CLI script.
Description	Freely selectable description of the CLI script.
Waiting time for reply	Waiting time for reply from the device in seconds. • Minimum value: 1 • Default value: 5 • Maximum value: 30
Universal	All devices can be assigned to jobs with this CLI script.
Restricted	Only devices whose article numbers were added using the "Article numbers" button can be assigned to jobs with this CLI script. CLI scripts with this compatibility type cannot be saved without specifying article numbers.

Parameter / control element	Function
Article numbers	Opens an editor in which article numbers of the devices for which the CLI script is valid can be added, changed and deleted.
CLI commands	Editor area for creating and editing CLI commands. There is no validation of the syntax of CLI commands. Each line is handled as a CLI command. A maximum of 50 CLI commands can be added. The following parameters can be used in CLI commands. The parameters are filled with the data of the device for which the CLI script is executed. Among other things, this allows the use of unique file names. • $I: IP address of the device The separators are removed in the parameter value, empty spaces are filled with "0". • $M: MAC address of the device The separators are removed in the parameter value. • $N: Name of the device. If the MAC address of the device or the name of the device is unknown, the relevant parameter is filled with the IP address of the device. Upper and lower case characters are not taken into account in the notation of the parameters.

4.4.9 Password strength

When a new password is assigned, the strength of this password is checked. In addition to the password length, SINEMA Server uses the following criteria to evaluate the strength of the password:

- The password contains an upper case letter.
- The password contains a lower case letter.
- The password contains a number.
- The password contains a special character. The following special characters are supported:
  [$/:?{-~!"^_`\\[

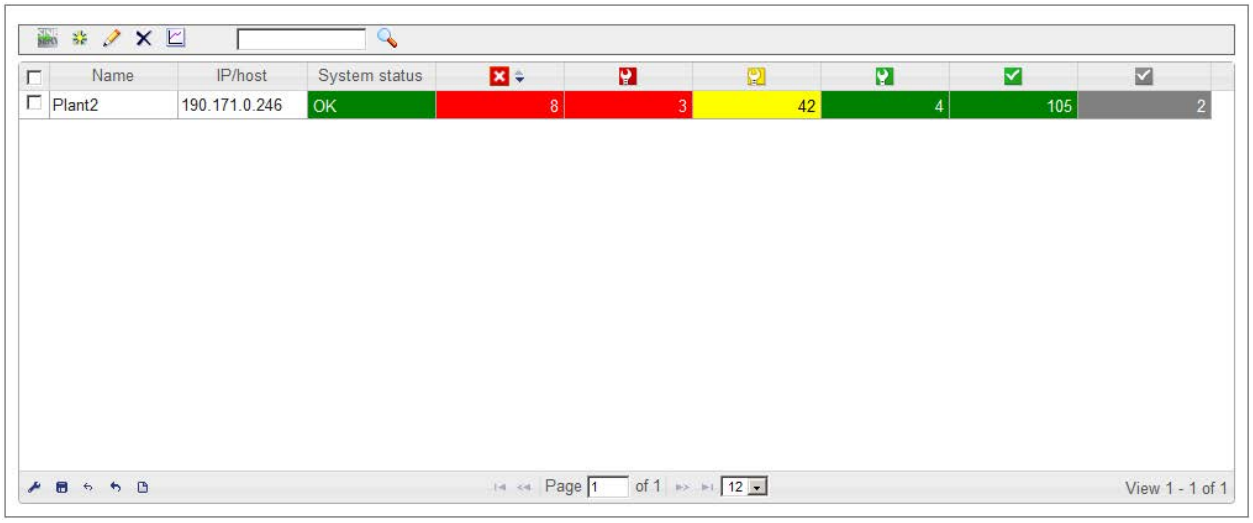
The password strength at hand is indicated by a correspondingly colored bar:

Password strength	Representation of the bar	Criteria for password strength
Weak		Password length < 9 characters (criteria are ignored) or Password length >= 9 characters, but no criterion is fulfilled.
		Password length >= 9 characters and one criterion is fulfilled.
Medium		Password length >= 9 characters and two criteria are fulfilled.
Strong		Password length >= 9 characters and three criteria are fulfilled.
		Password length >= 9 characters and four criteria are fulfilled.

4.5 Server overview

You can open the "Server overview" Web page in one of the following ways:

- Entry in the navigation bar
- Entry below the "Server overview" node in the device tree



Meaning

On the "**Server overview**" Web page, SINEMA Server provides an overview of the overall statuses of devices monitored by other SINEMA Server instances in the network. To do this, the Web page shows how many devices have which overall status for each SINEMA Server. To increase and decrease the number of devices, there are system events that can be enabled or disabled for each device overall status.

Before SINEMA Server instances are displayed on this Web page, they must be created and configured using the button, refer to the section "Configuring a SINEMA Server instance".

Configured SINEMA Server instances can be called directly from the server overview. When they are called up, there is an automatic authentication with the user data with which the calling user is logged in for the local SINEMA Server instance. To do this, the user needs the "Server access via URL" right.

Operator input

The following table shows the operator control elements of the "Server overview" Web page with a brief explanation.

Icon	Display / function
	Open server in new tab With this function, you open the selected SINEMA Server instance and are automatically logged in with the user data configured for the instance in the server overview.
	Add new server This function opens the "SINEMA Server editor" dialog. In this dialog, you configure the data for the reachability of the SINEMA Server instance; refer to the section "Configuring a SINEMA Server instance".
	Edit selected server With this function you open the "SINEMA Server editor" dialog in which you can edit the existing entries, refer to the section "Configuring a SINEMA Server instance".
	Delete servers
	Create report With this function, you open the dialog for configuring a report containing the the number of overall statuses of devices monitored by a selected SINEMA Server instance. The following parameters can be configured in this dialog: • The period the report will cover. • The overall device statuses to be included in the report.
	Enter text for text search / filter
	Start text search / filter setting

Content

The following information is available in the columns of the server overview:

Parameter	Meaning
Name	Name of the SINEMA Server instance
IP/host	IP address of the SINEMA Server instance
System status	Reachability status of the SINEMA Server instance
	Number of devices that currently have the overall status "Not reachable".
	Number of devices that currently have the overall status "Error".
	Number of devices that currently have the overall status "Maintenance demanded".
	Number of devices that currently have the overall status "Maintenance required".
	Number of devices that currently have the overall status "OK".
	Number of devices that currently have the overall status "Not connected".
Port Web UI	Port used to call the SINEMA Server instance from the server overview.

Parameter	Meaning
Protocol	Protocol used to call the SINEMA Server instance from the server overview.
Port server poll	Port used to poll the overall device statuses from the SINEMA Server instance.

Note

User-specific display of the SINEMA Server instances

SINEMA Server instances that were created in the server overview can be part of views that can be assigned to specific users. If you are logged in as a user whose user group has restricted user rights and to which such a view was assigned, you will only see the SINEMA Server instances of the corresponding view in the server overview.

Configuring a SINEMA Server instance

The "Basic settings" tab of the "SINEMA Server editor" window contains the following operator control elements:

Operator control element	Function
Name	Name of the SINEMA Server instance to be displayed in the server overview
IP/host	IP address of the SINEMA Server instance
Protocol	Protocol used to call the SINEMA Server instance from the server overview.
Port	Port used to call the SINEMA Server instance from the server overview.

In the "Advanced settings" tab, the port used to poll the device overall statuses from the SINEMA Server instance can be configured.

Note

Shared secret required

Before a SINEMA Server instance can query device data of another SINEMA Server instance and display it in the server overview, the same shared secret must be configured for both of them i "Administration > System > Configuration, refer to the sectionAdministration - System configuration (Page 212) .

Calling up a SINEMA Server instance - requirement

SINEMA Server instances are called up from the server overview using the HTTPS protocol. To be able to call up SINEMA Server instances, you first need to install the server certificate on your client.

Follow the steps outlined below:

1. In your Web browser, click the "Certificate error" notification.

   This opens a dialog with a message regarding the non-trustworthy certificate.

2. Click the "Show certificate" button.

   The certificate window opens.

3. Select the "Install certificate" option and follow the instructions to install the certificate of the relevant server on your client computer.

See also

SINEMA Server users and roles concept (Page 66)

Data exchange via OPC

5

5.1 Access via OPC server - options and concept

OPC

The OPC standard (Open Process Control) is used for devices in industrial automation to transfer plant data, alarms and events, historical data and data from batch processes between control devices of different manufacturers in real time. The OPC interface is a standard for the co-operation of differing systems when exchanging data at runtime. Systems of other manufacturers can be connected to the OPC server via OPC clients and read out or monitor the data.

When accessing data, the following types of access must be distinguished:

- Data access with OPC (UA)

  The OPC UA (Unified Architecture) is based on a service-oriented architecture and manages without the components of the Microsoft COM/DCOM (Component Object Model/Distributed Object Component Model).

- Data access with OPC (DA)

  OPC DA is a standard with specifications for real-time data transfer from data acquisition devices such as PLCs. It is used to provide a display and interface for devices such as HMI devices. SINEMA Server supports the range of functions of OPC DA.

  With OPC DA remote access, the DCOM settings must be configured in SINEMA Server.

Accessing SINEMA Server data via OPC

The data of the devices that were made visible in OPC in "Administration > Monitoring > OPC" exist on the OPC server. This data can be accessed by any OPC client.

As default, access to the OPC UA server is only possible with user authentication. You can disable this presetting in the "Port settings" tab of SINEMA Server Monitor.

In the case of changes to the OPC visibility of devices, all connected OPC clients must be disconnected and reconnected to the OPC Server so that the changes are visible for the OPC clients.

5.2 Data access with OPC (UA)

The OPC UA (Unified Architecture) is based on a service-oriented architecture and manages without the components of the Microsoft COM/DCOM (Component Object Model/Distributed Object Component Model). OPC UA is a cross-platform standard with which systems and devices of different types can communicate with each other. They send messages between clients and servers via different types of network. UA supports rugged, secure communication that protects the identity of servers and clients and provides protection from attacks.

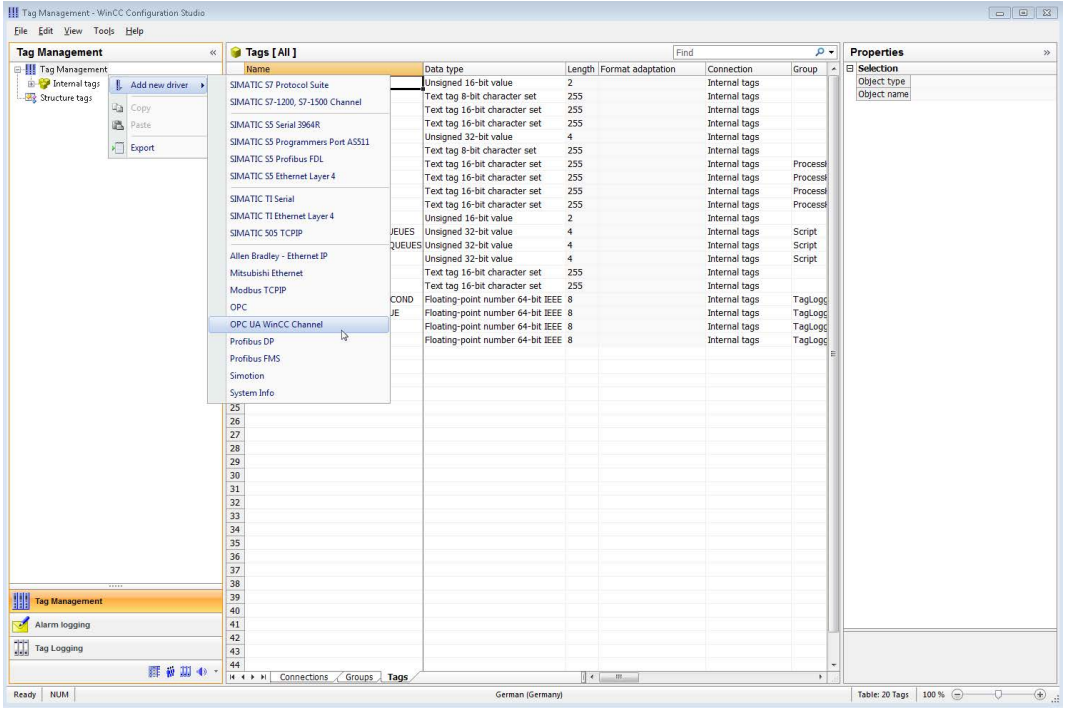
Configuring UA ports

The default port used for a UA server is 4841. This port can be configured using the configuration option in the shortcut menu of the "SINEMA Server Monitor" sub window. To access this shortcut menu, right click on the icon for the sub window "SINEMA Server Monitor" in the Windows system tray. A window with a list of options is then displayed.

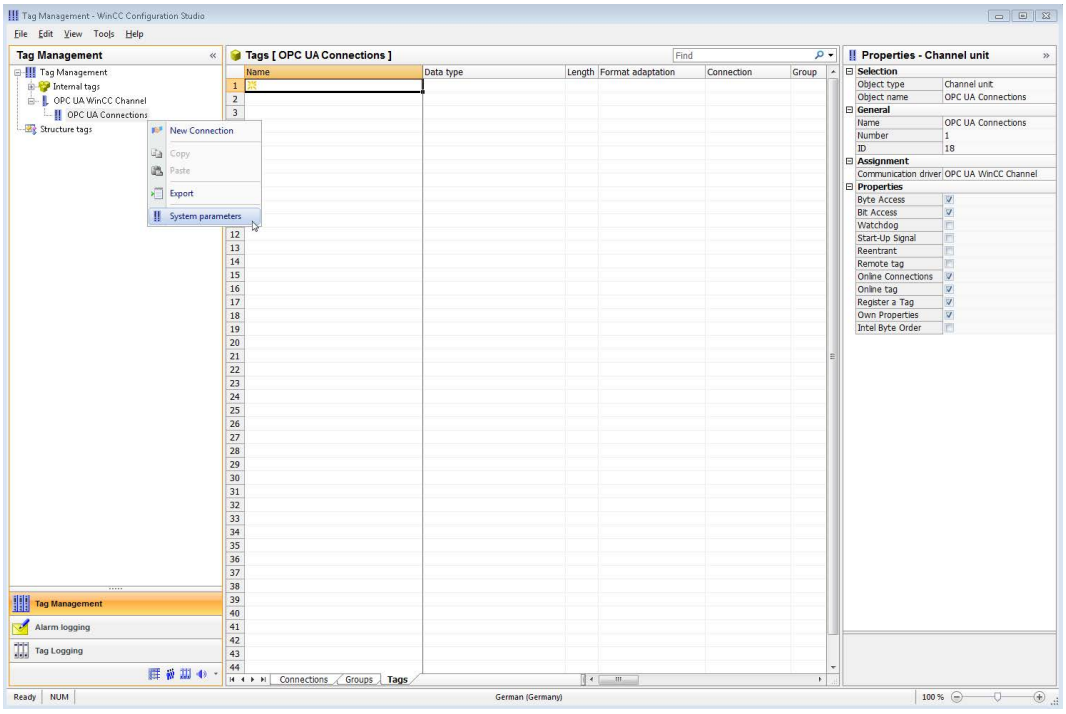
If OPC UA server and OPC UA client are separate PCs, the OPC UA port used must be open in the firewall of both PCs. For more information, refer to section Port settings (Page 32).

OPC UA access with WinCC Explorer 7.4

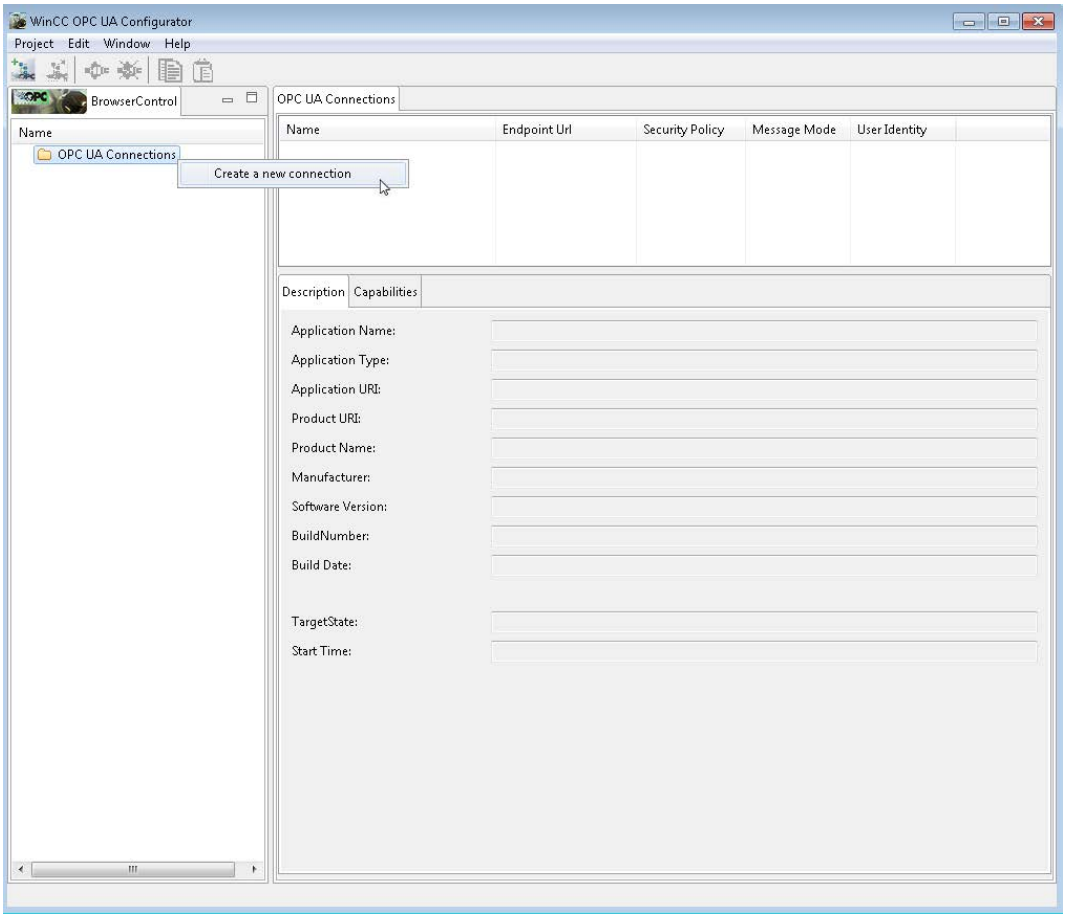
1. Start SINEMA Server.
2. Start the WinCC Explorer.
3. Open the Tag Management.
4. In the shortcut menu of the entry "Tag Management" select the menu command "Add new driver > OPC UA WinCC Channel".



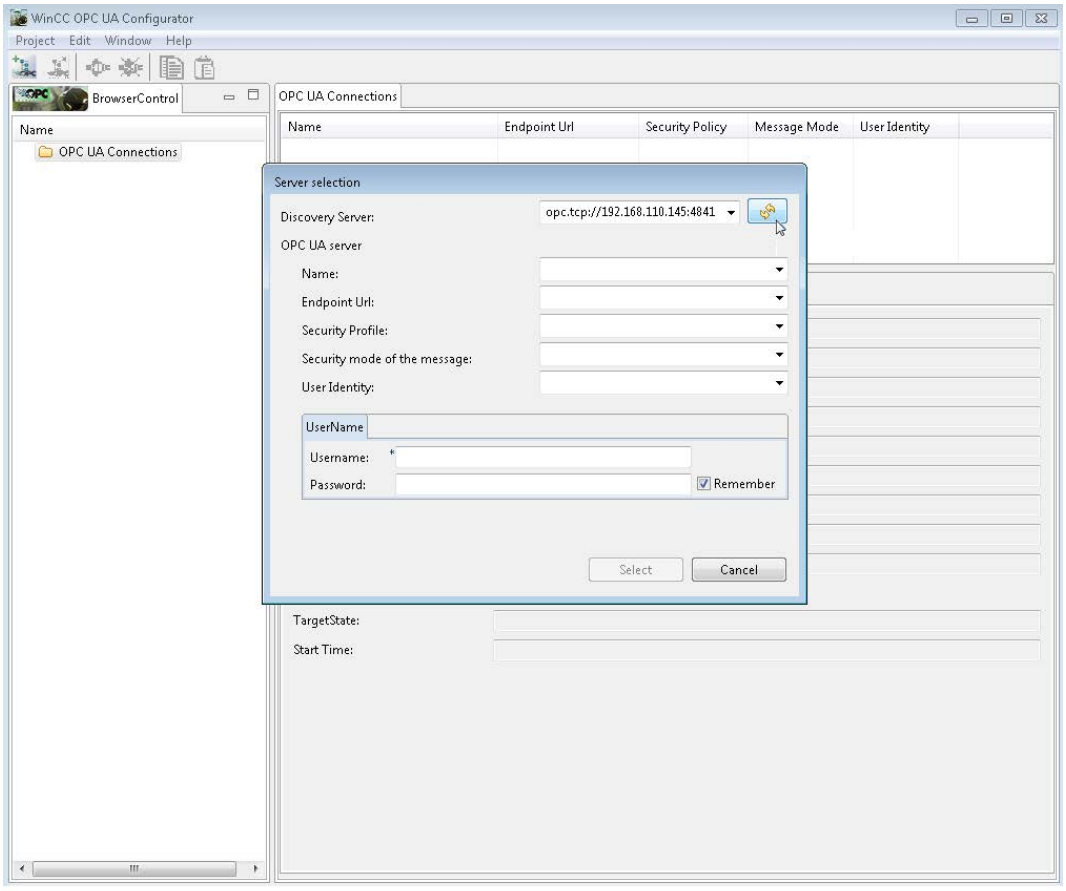
5. In the shortcut menu of the entry "OPC UA Connections" select the entry "System parameters".



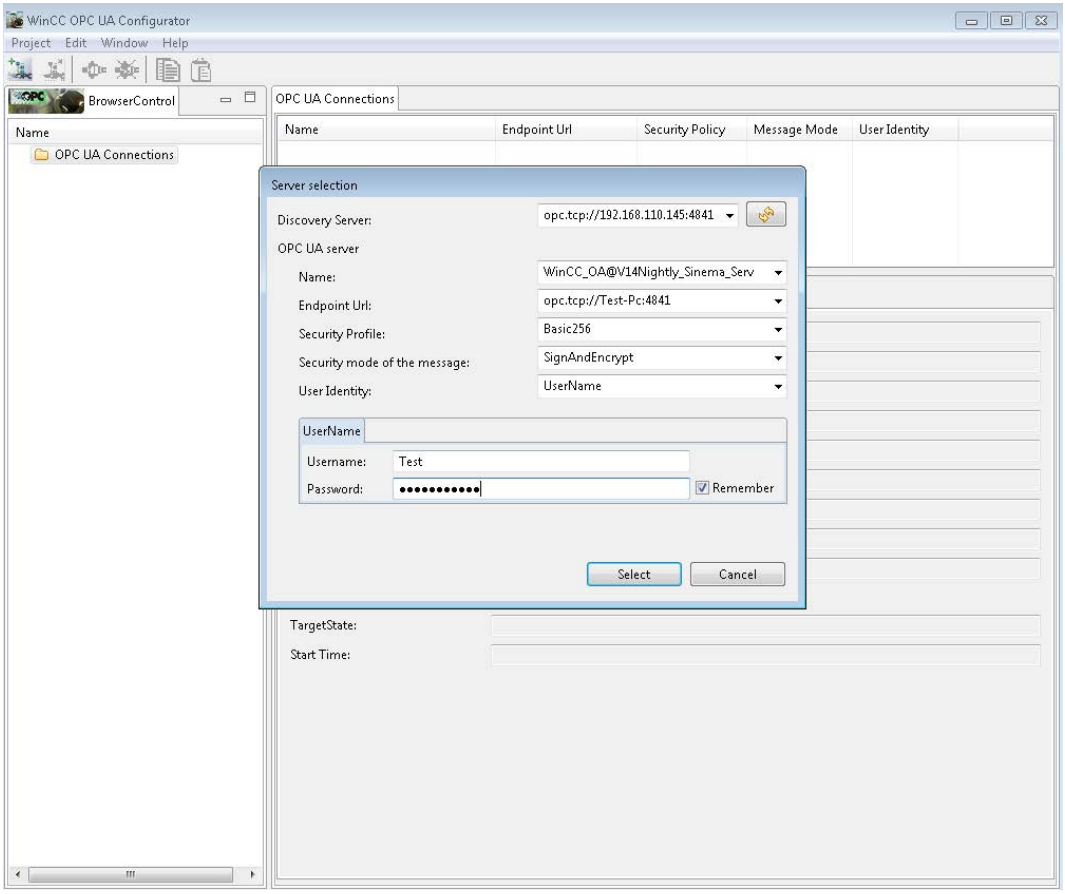
6. In the WinCC OPC UA Configurator in the shortcut menu of the entry "OPC UA Connections" select the menu command "Create a new connection".



7. In the window "Server selection" enter the data of the OPC UA server in the input box "Discovery Server" and click on the button to update the window.



8. As default, access to the OPC UA server is only possible with user authentication. For this reason for the parameter "User Identity" select the entry "UserName" and enter the data of a user that exists in SINEMA Server.

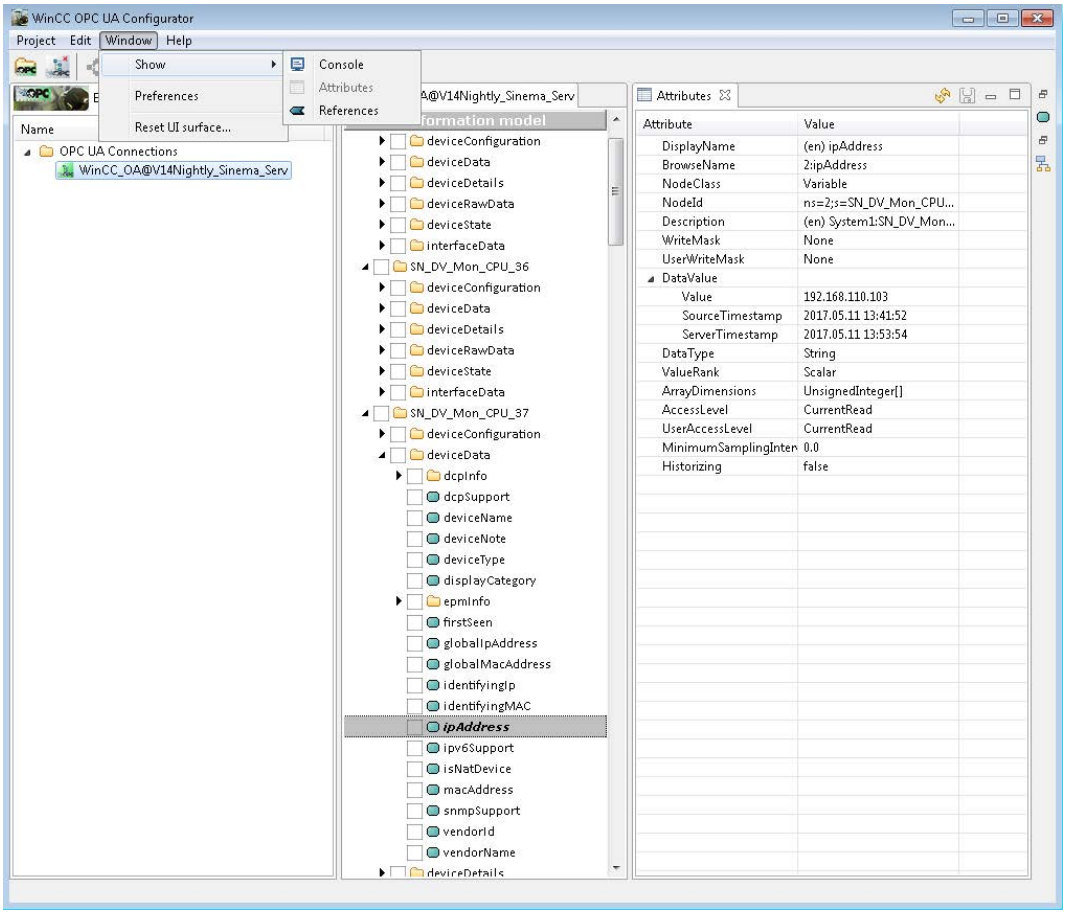


You can disable this presetting for user authentication when accessing the OPC UA server in the "Port settings" tab of SINEMA Server Monitor.

Result: The connection establishment initially fails, because created certificates are rejected as default by the OPC UA server. The entry for the OPC UA connection turns red.

9. Move the rejected certificates on the OPC UA server from the directory "C:\Siemens\SINEMAServer\WinCC_OA\3.14\data\opcua\server\PKI\CA\rejected" to the directory "C:\Siemens\SINEMAServer\WinCC_OA\3.14\data\opcua\server\PKI\CA\certs".

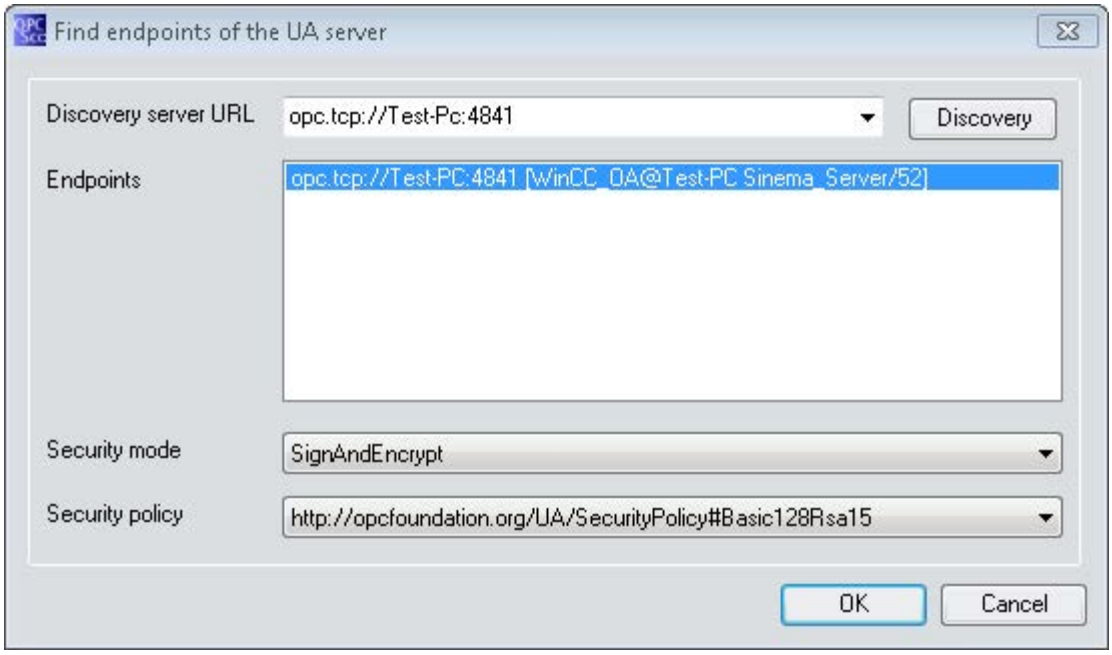
Result: Youi have set up a connection to the OPC UA server. With the menu command "Window > Show > Attributes" the SINEMA Server data can be displayed.



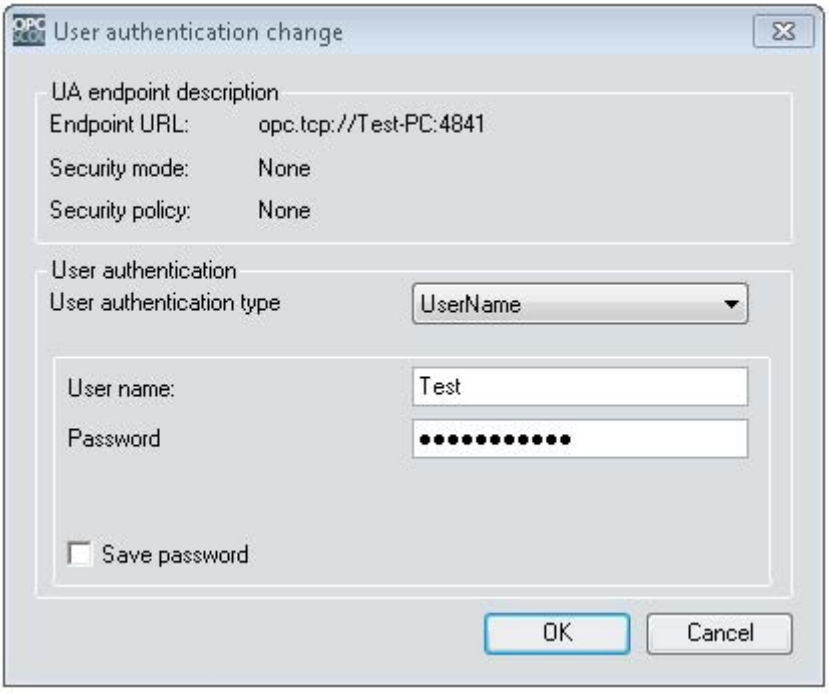
OPC UA access with OPC Scout

1. Start SINEMA Server.
2. Start OPC Scout V10.

3. Create a signed and encrypted UA server connection in OPC Scout V10 (opc.tcp://pcname:port).

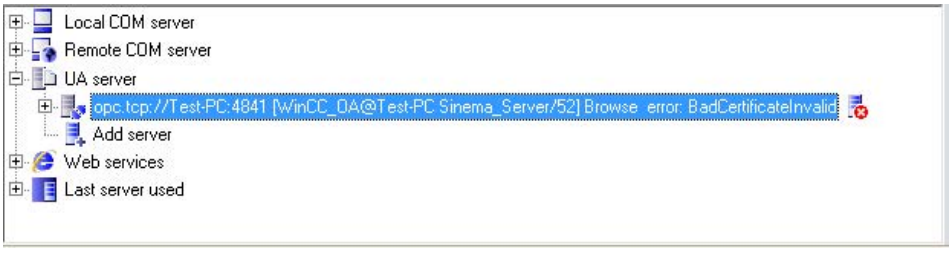


4. As default, access to the OPC UA server is only possible with user authentication. For this reason right-click on the server, select the menu command "Change user authentication", from the drop-down list "User authentication type" select the entry "UserName" and enter the data of a user that exists in SINEMA Server.



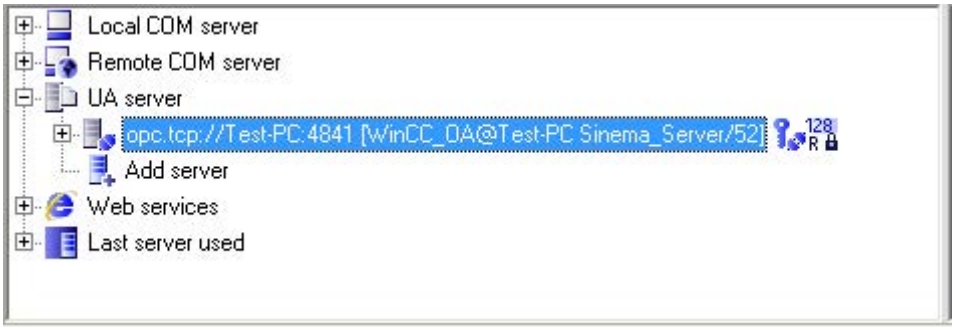
You can disable this presetting for user authentication when accessing the OPC UA server in the "Port settings" tab of SINEMA Server Monitor.

5. Double-click on the server so that the error message "Bad certificate error" appears.



6. You will now find the rejected OPC Scout V10 certificate in the directory "C:\Siemens\SINEMAServer\WinCC_OA\3.14\data\opcua\server\PKI\CA\rejected".

7. Move this certificate to the folder "C:\Siemens\SINEMAServer\WinCC_OA\3.14\data\opcua\server\PKI\CA\certs".
8. Now double-click on the server again for a signed and encrypted connection.



5.3 Data access with OPC (DA)

5.3.1 Configuring Windows settings

Adding Windows users

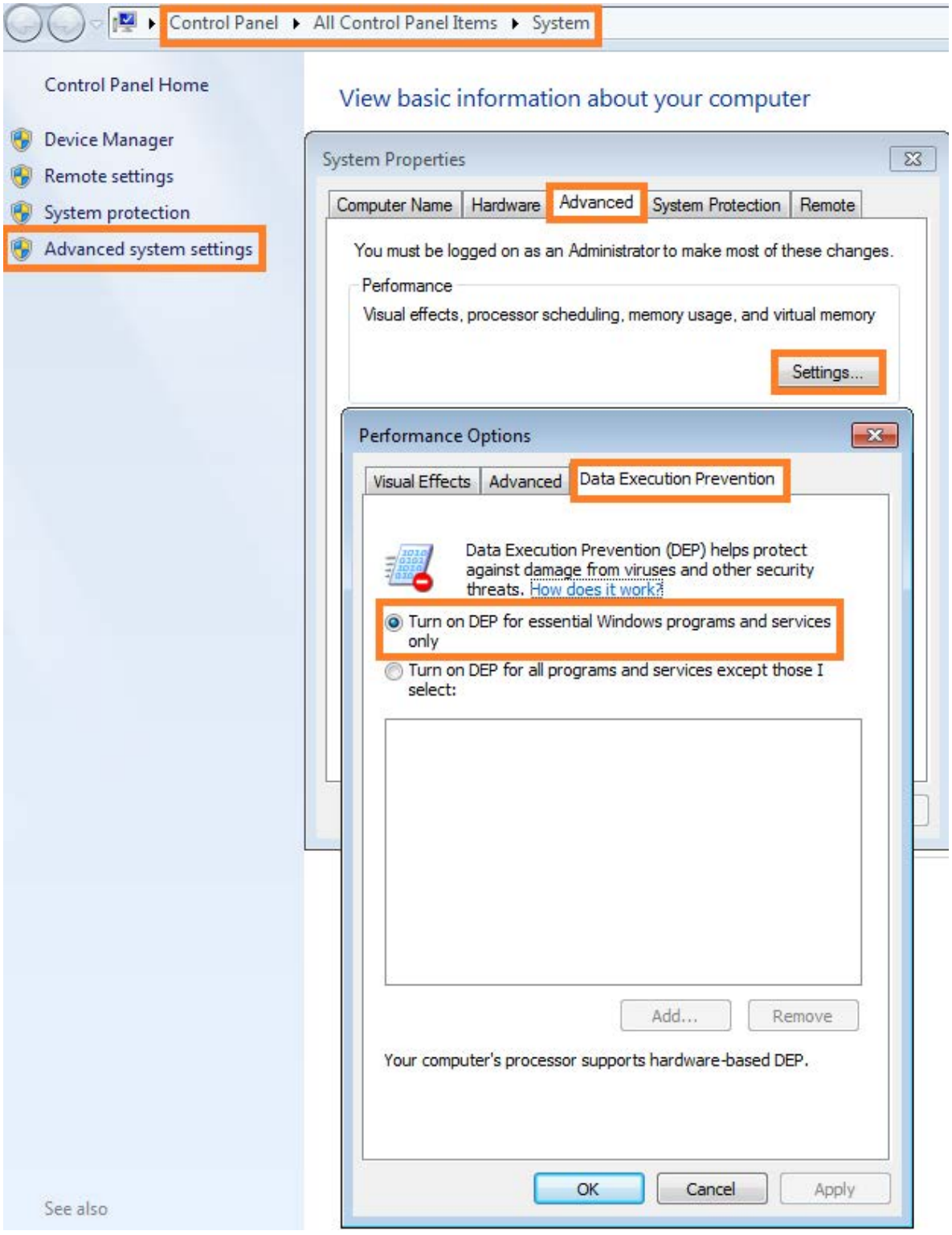
Add a new Windows user with administrator rights. The same user with the same password must exist on the OPC DA client.

Enabling data execution prevention

By default, data execution prevention is enabled for all programs. If it is disabled, proceed as follows:

1. Select the "Advanced" tab under "Control Panel > System and Security > System > Advanced System Settings".
2. Click on the "Settings..." button in the "Performance" area.

3. Select the "Data Execution Prevention" tab.
4. Ensure the "Turn on DEP for essential Windows programs and services only" option button is selected.



5.3.2 Configuration of the DCOM settings on the management station

Overview

The configuration of the DCOM settings comprises the following steps:

- Configuration in workgroup mode with the "OPC DA User" user group and the users "Alpha" and "Beta"
- Configuration of the "OPC DA User" user group
- Configuration of the default DCOM settings
- Configuration of the DCOM settings for OPC servers
- Configuration of the DCOM settings for the OPC server browser

Configuration in workgroup mode with the "OPC DA User" user group and the users "Alpha" and "Beta"

Example of workgroup mode

The "Alpha" user is logged on to the PC with the OPC DA server, the "Beta" user to the PC with the OPC DA client. For DCOM operation, you now need to create a "Beta" account on the server PC (with the same password as on the client PC) and an "Alpha" account (same password) on the client PC.

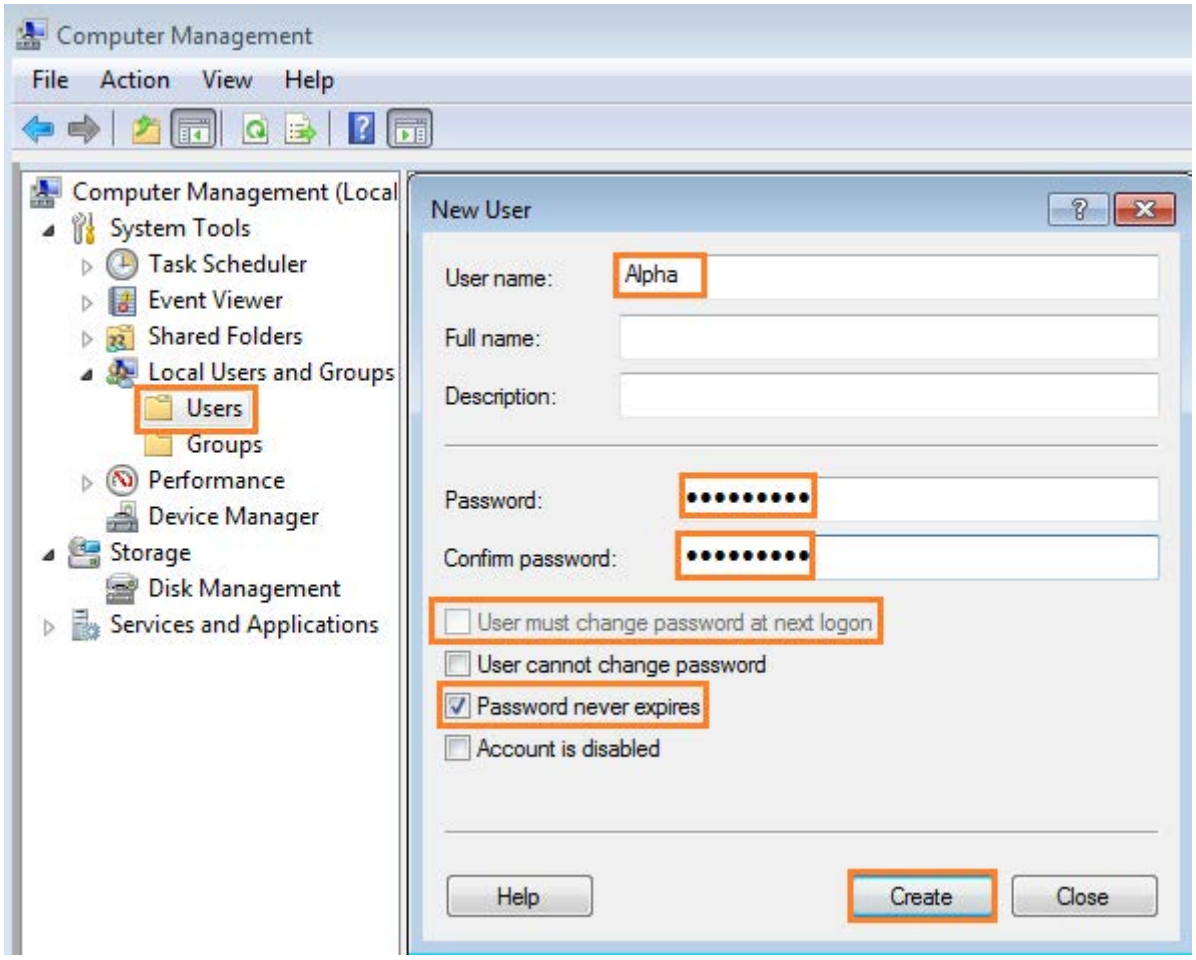
We recommend creating an "OPC DA User" user group with the users "Alpha" and "Beta" for the desired users of SINEMA Server OPC DA server.

Configuration of the "Alpha" and "Beta" users

Follow the steps below:

1. Select the "Manage" command in the shortcut menu of the navigation entry under "Start > Computer".
2. Select the "System > Local Users and Groups > Users" entry.
3. Select "New user..." from the shortcut menu of the entry.

4. In the "New User" dialog, enter the user name "Alpha". Enter a password of your choice in the "Password" box and confirm it. Clear the check box "User must change password on next logon" and select the check box "Password never expires". Then click the "Create" button.



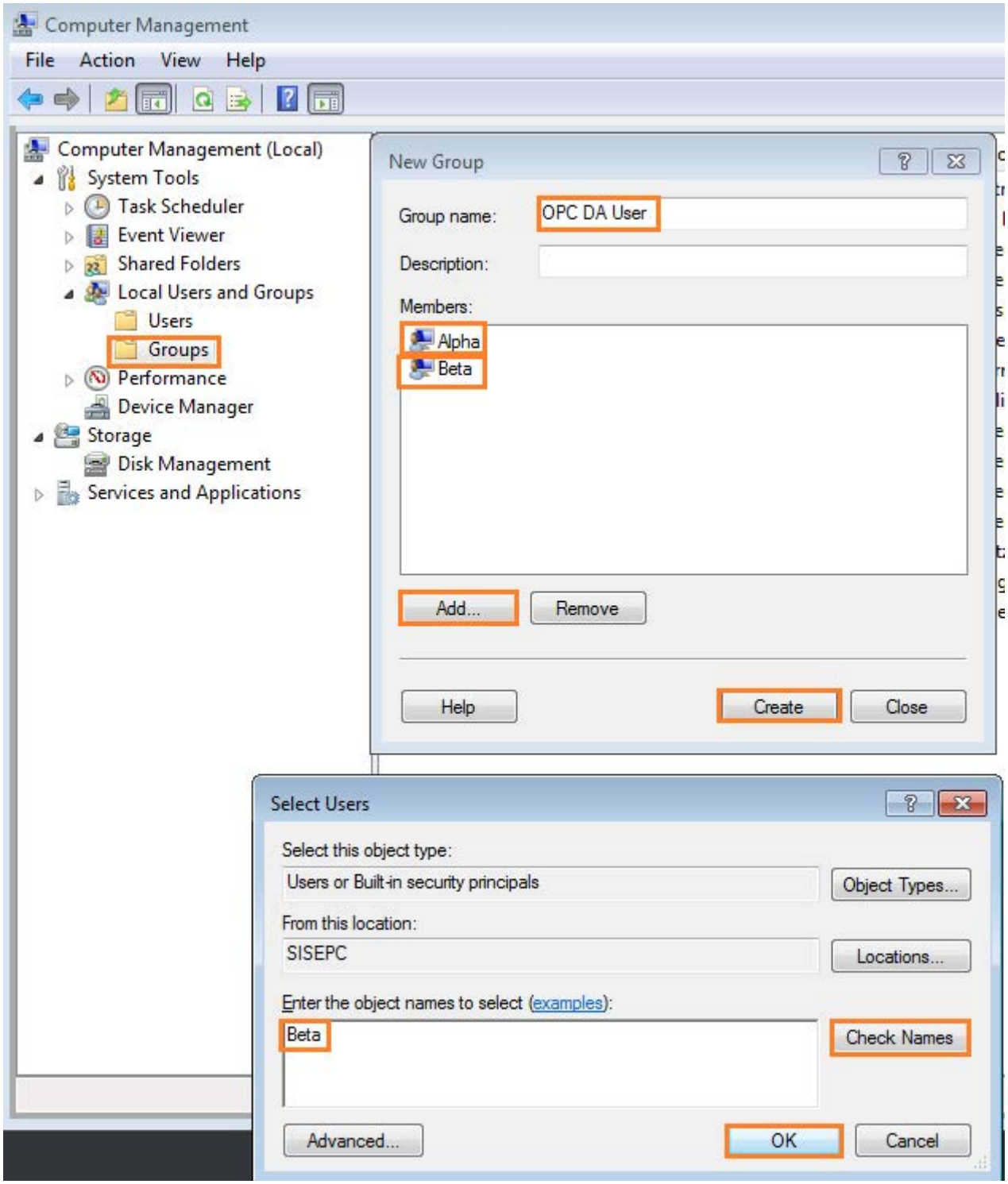
5. Create a "Beta" user using the same method.

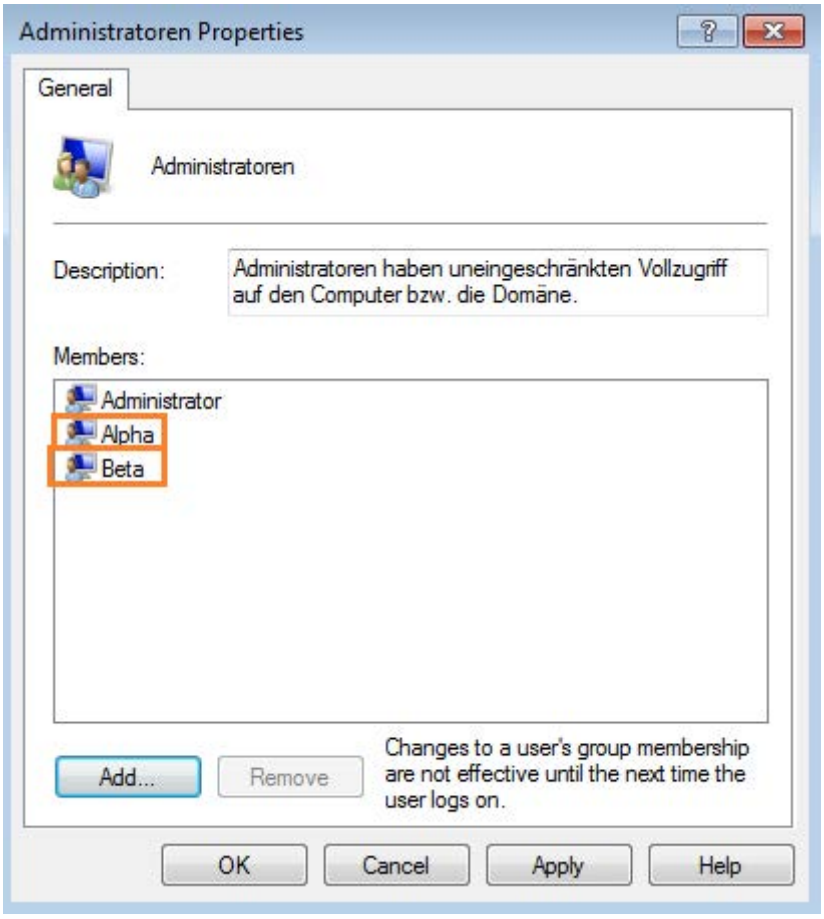
Configuration of the "OPC DA User" user group

Follow the steps below:

1. Select the "Manage" command in the shortcut menu of the navigation entry under "Start > Computer".
2. Select the "System > Local Users and Groups > Groups" entry.
3. Select "New group..." from the shortcut menu of the entry.
4. In the "Group name" box, enter the group name "OPC DA User".
5. Click the "Add..." button.

6. Add the desired DCOM users "Alpha" and "Beta" to the "OPC DA User" group and the "Administrators" group.



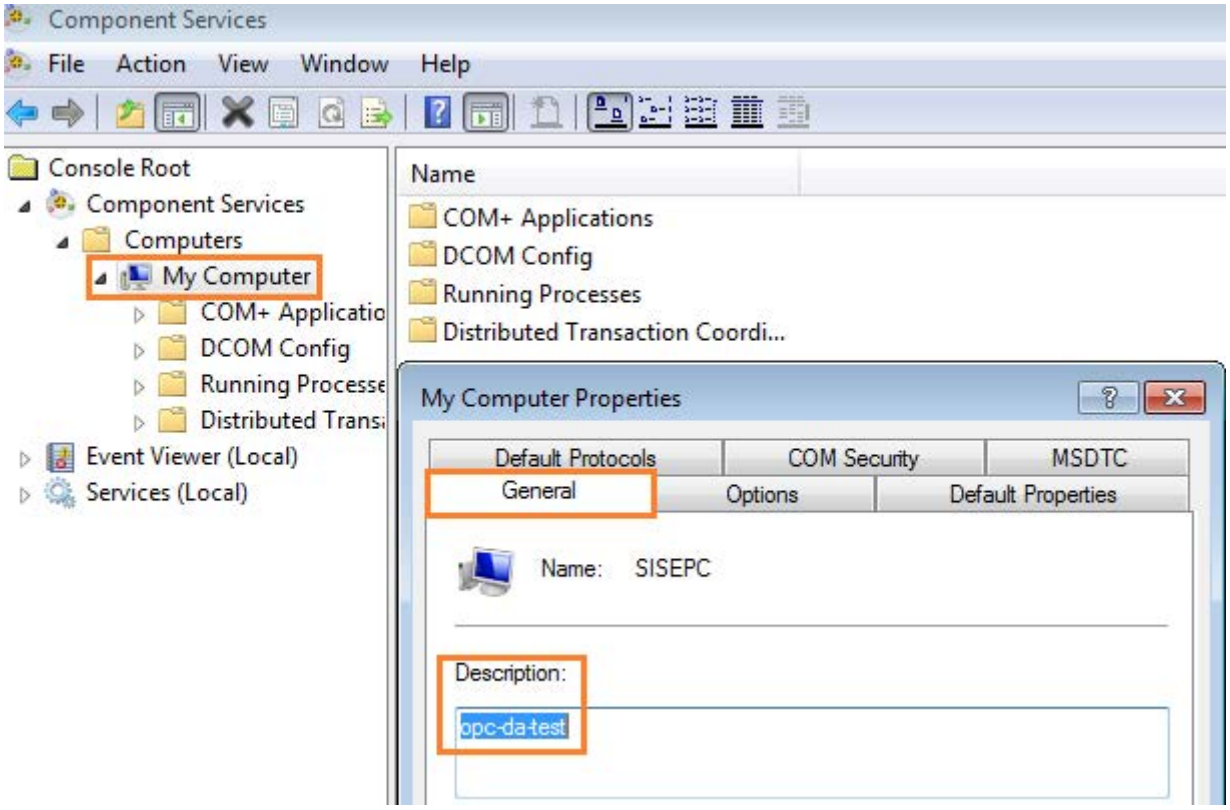


7. The "OPC DA User" group can now be selected by the OPC DA COM server for start and access permissions for DCOM configuration.

Configuration of the default DCOM settings

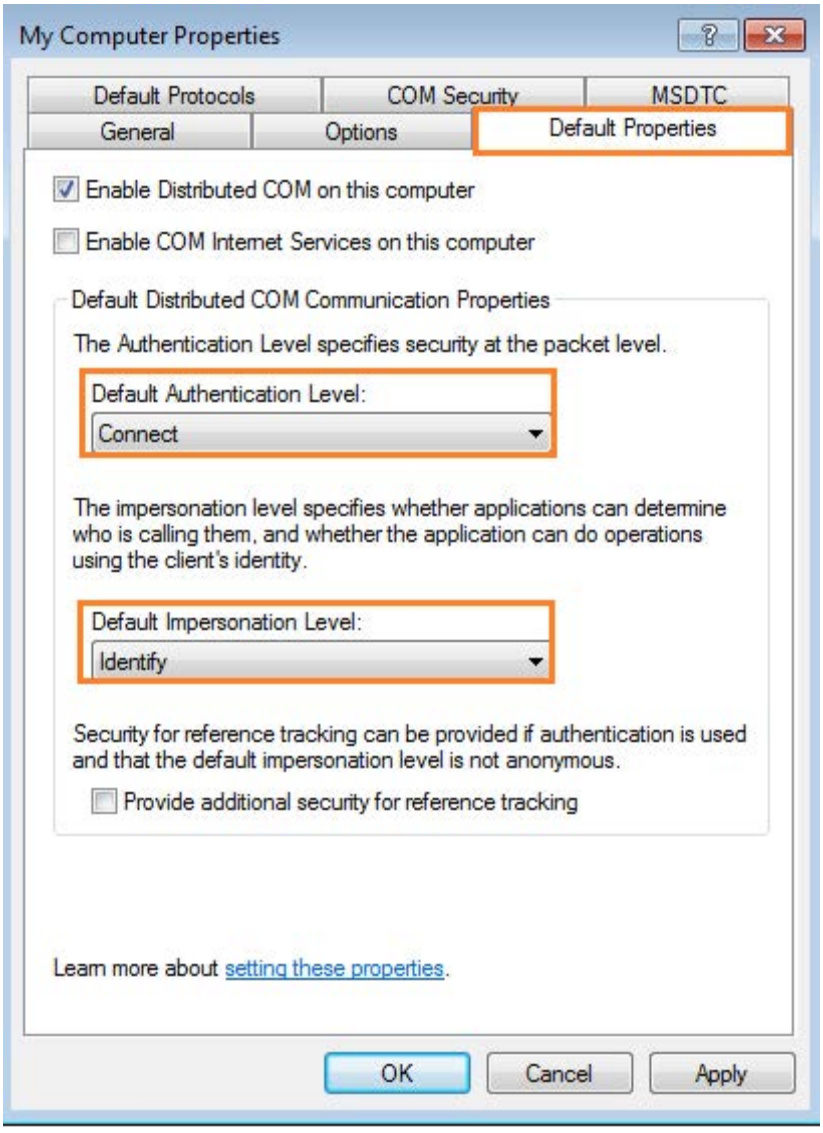
1. Select the "Start > Run" menu command.
2. Enter the string "dcomcnfg" in the input box and click "OK".
3. Select the "Component Services > Computer > My Computer" node in the area on the left.
4. Select the shortcut menu command "Properties".

5. Enter a description and click the "Apply" button.



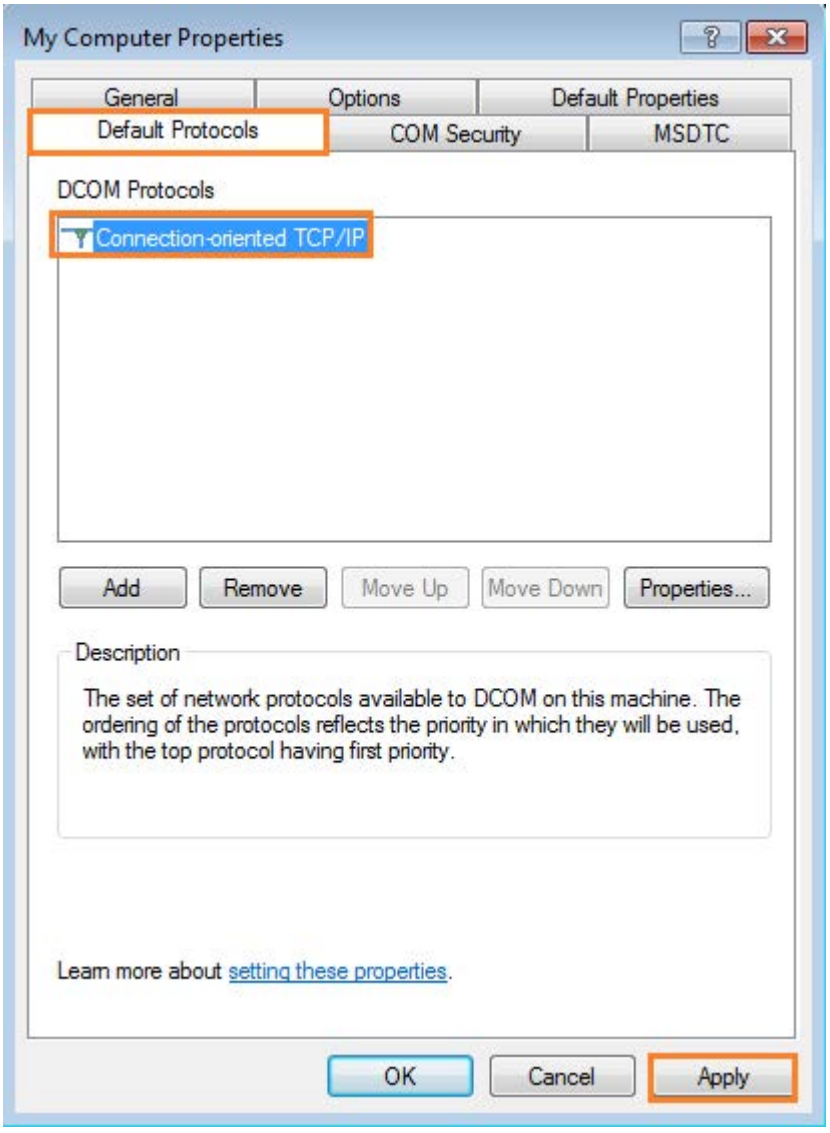
6. Select the "Default Properties" tab.

7. Select the default authentication level "Connect" and the default impersonation level "Identify" and click the "Apply" button.



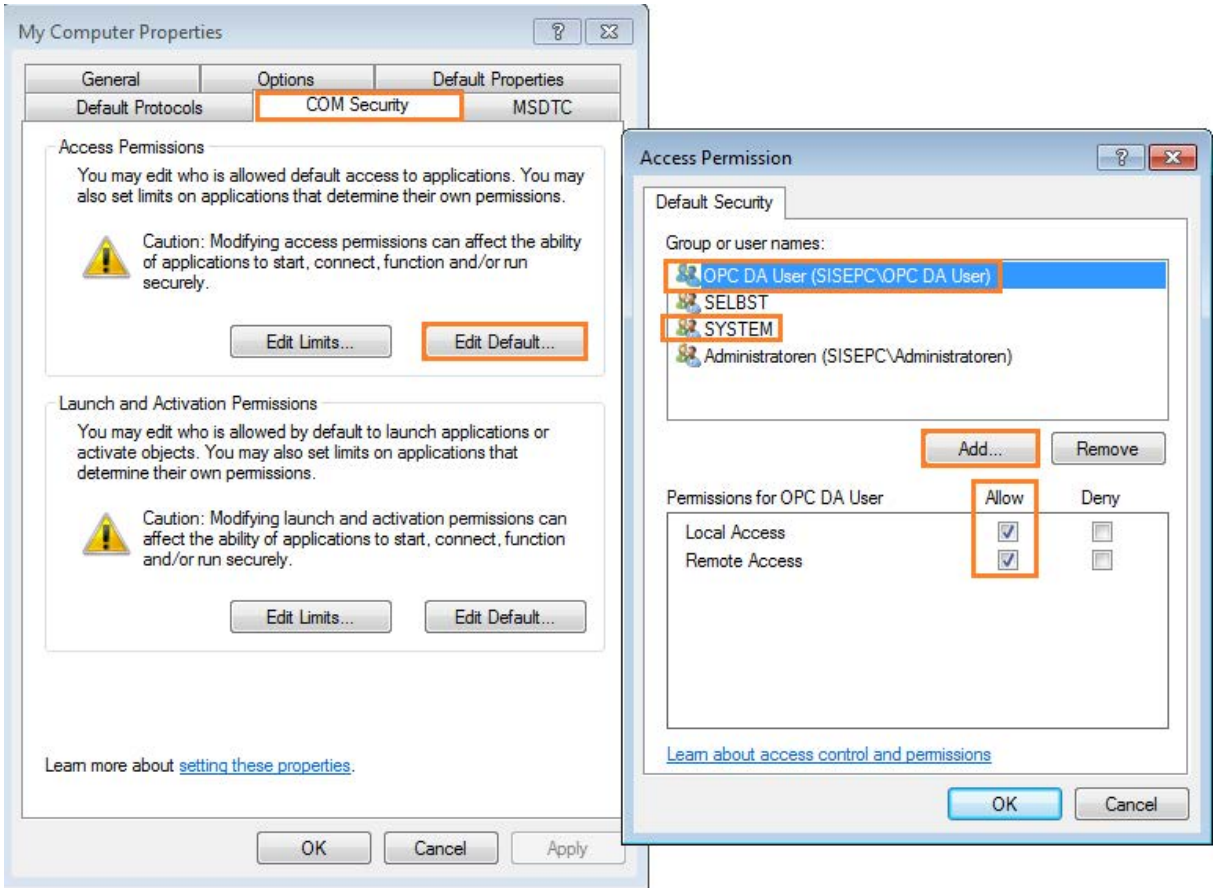
8. Select the "Default Protocols" tab.

9. Move the "Connection-oriented TCP/IP" entry to the first position in the list, remove other unused protocols and click the "Apply" button.



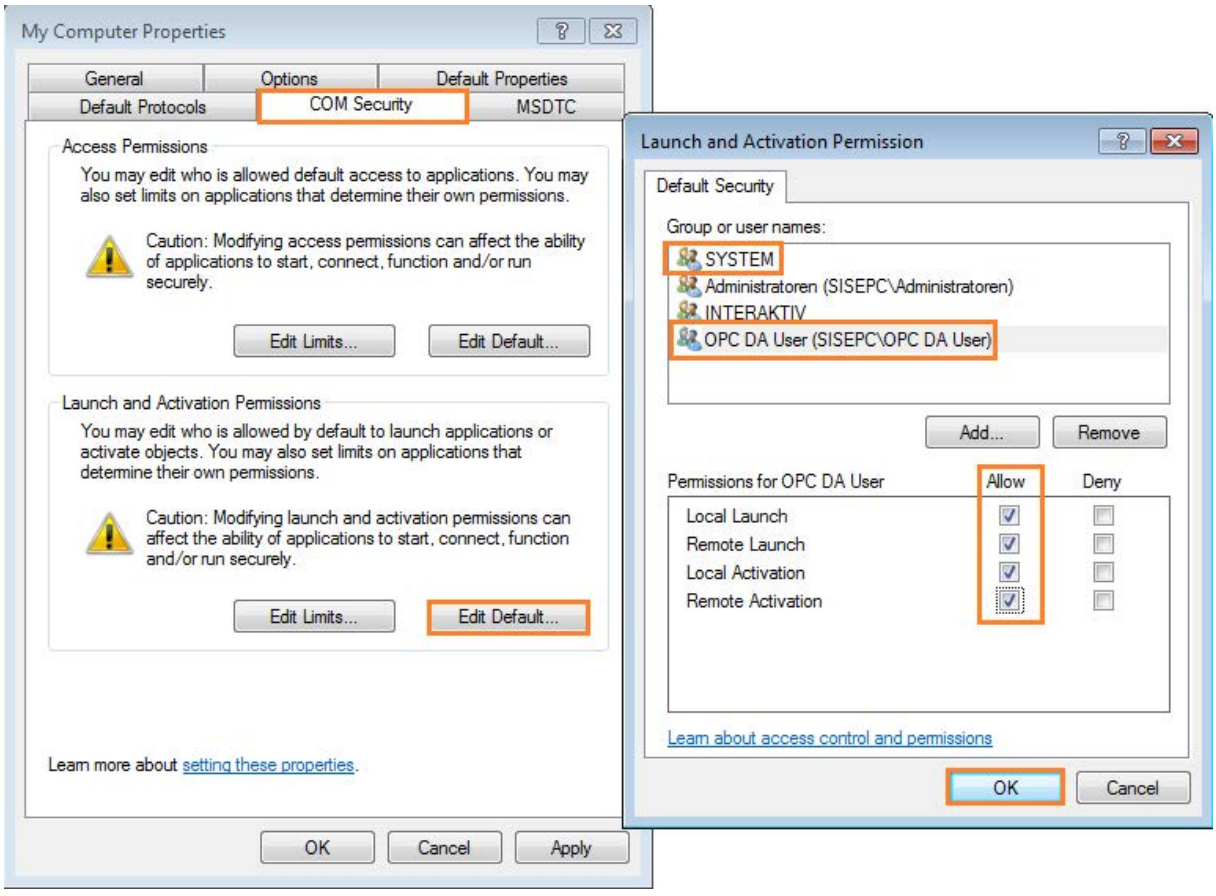
10. Select the "COM Security" tab.
11. Click on the "Edit Default..." button in the "Access Permissions" area.
12. Configure the access permissions for the OPC server and the OPC server browser according to your requirements. Add the "OPC DA User" user group and assign the "Local Access" and "Remote Access" permissions.

13. Make sure that local and remote access is allowed for the "SYSTEM" group. If this group does not exist, add it using the "Add..." button. Confirm the configuration of the access permissions with "OK".
    Result: All users of the "OPC DA User" group have local access and remote access to the OPC server and OPC server browser.



14. Click on the "Edit Default..." button in the "Launch and Activation Permissions" area.

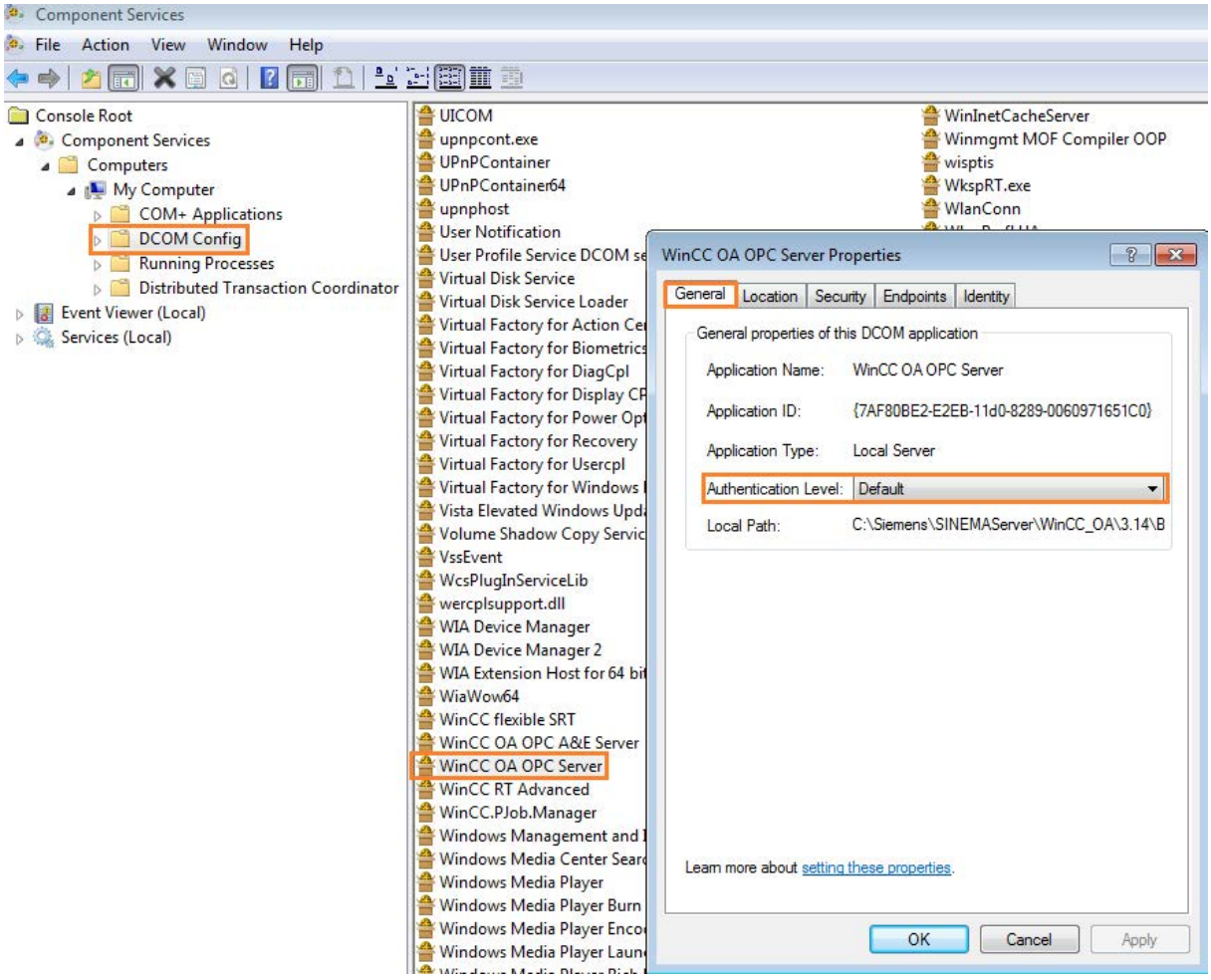
15. Repeat steps 12 and 13 and also add the "OPC DA User" user group and the "System" user with local and remote access rights.
16. Confirm the configuration of the access permissions with "OK".



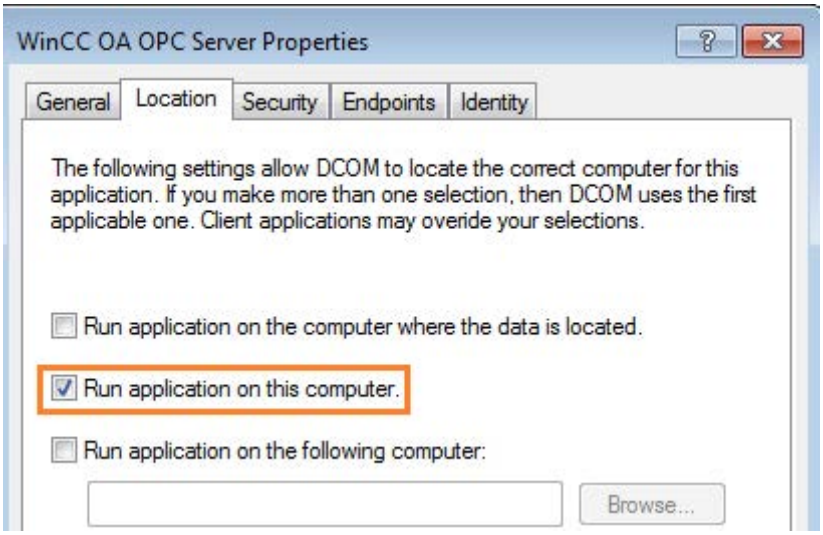
Configuration of the DCOM settings for OPC servers

1. Select the "Start > Run" menu command.
2. Enter the string "dcomcnfg" in the input box and click "OK".
3. Select the "DCOM Config" node in the "Component Services" window under "Component Services > Computer > My Computer".
4. Select the "WinCC OA OPC Server" entry in the middle area of the page.
5. Select the "Properties" entry in the shortcut menu.

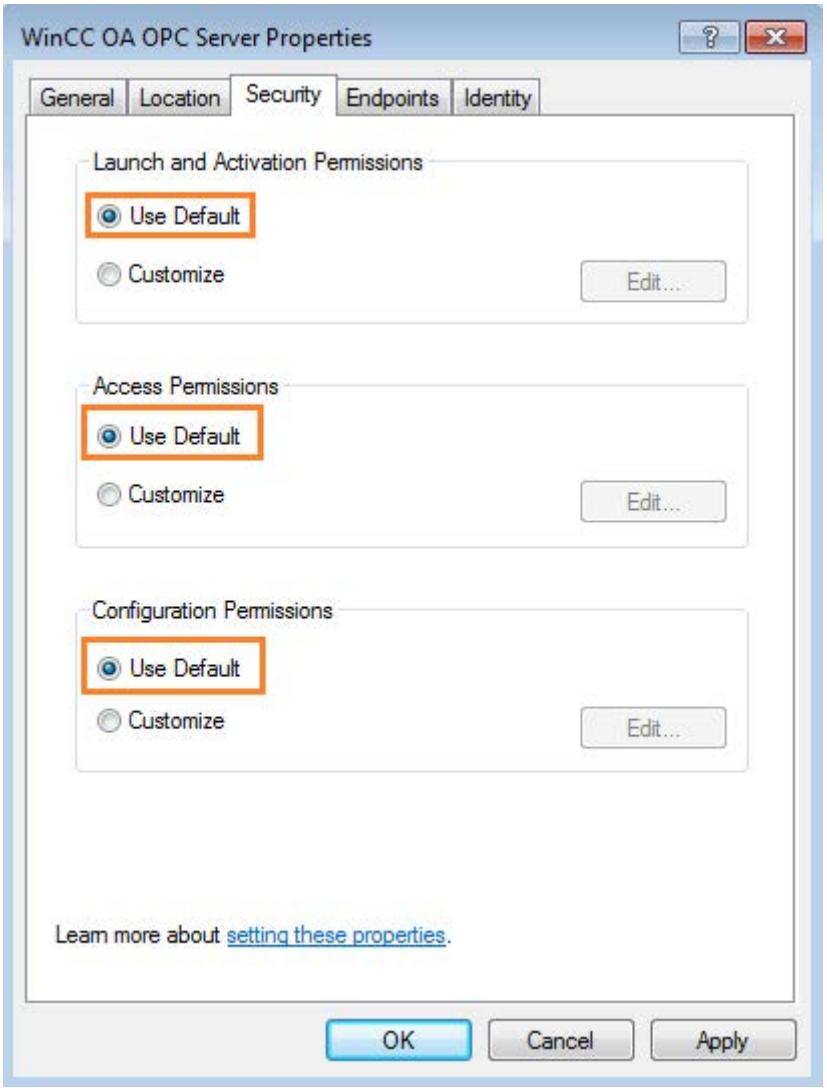
6. Select the "Default" authentication level in the "General" tab.



7. In the "Location" tab, select the "Run application on this computer" check box and click the "Apply" button.

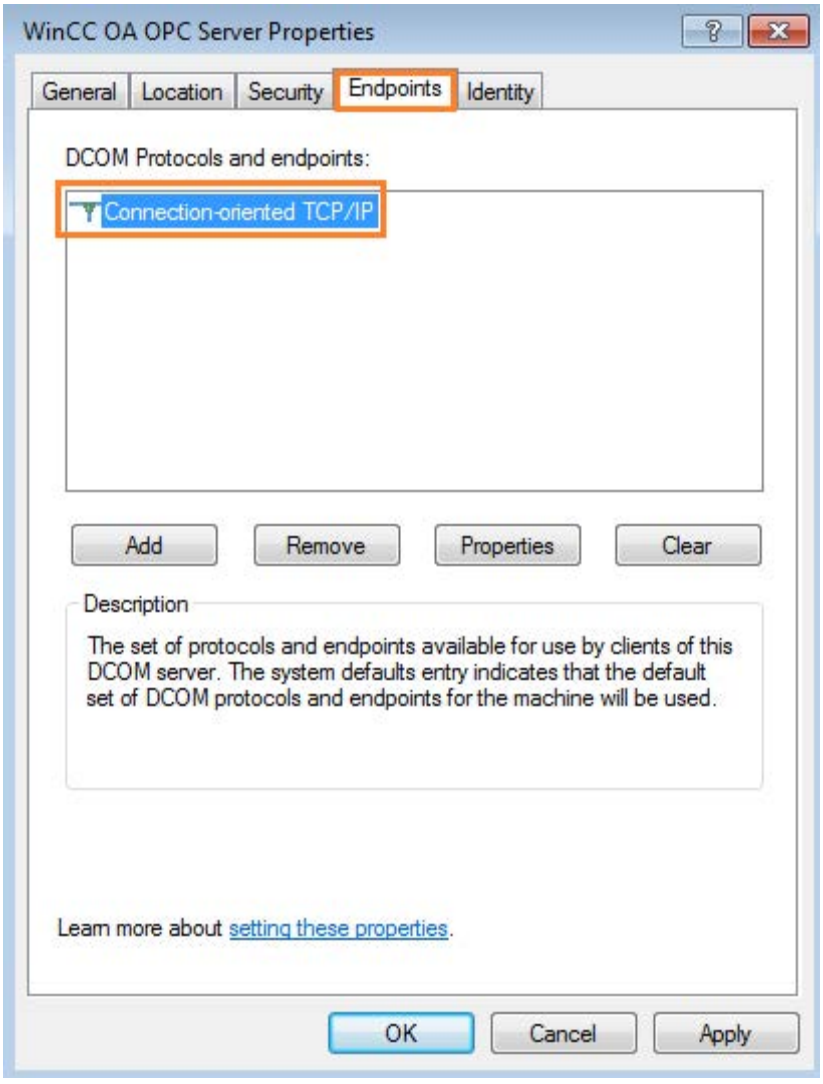


8. Select the "Security" tab.
9. In the "Launch and Activation Permissions", "Access Permissions" and "Configuration Permissions" areas, select the "Use default" option button or select suitable OPC server users and/or groups.

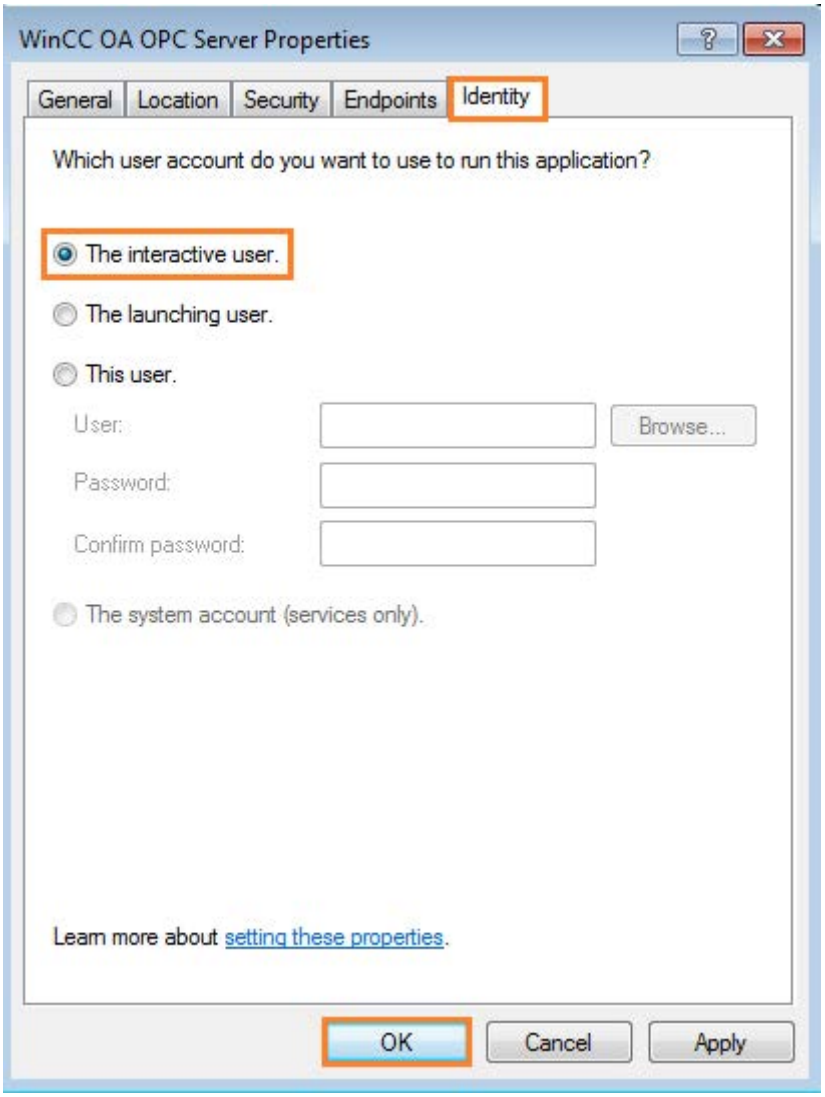


10. Select the "Endpoints" tab.

11. Move the "Connection-oriented TCP/IP" entry to the first position in the list, remove other unused protocols and click the "Apply" button.



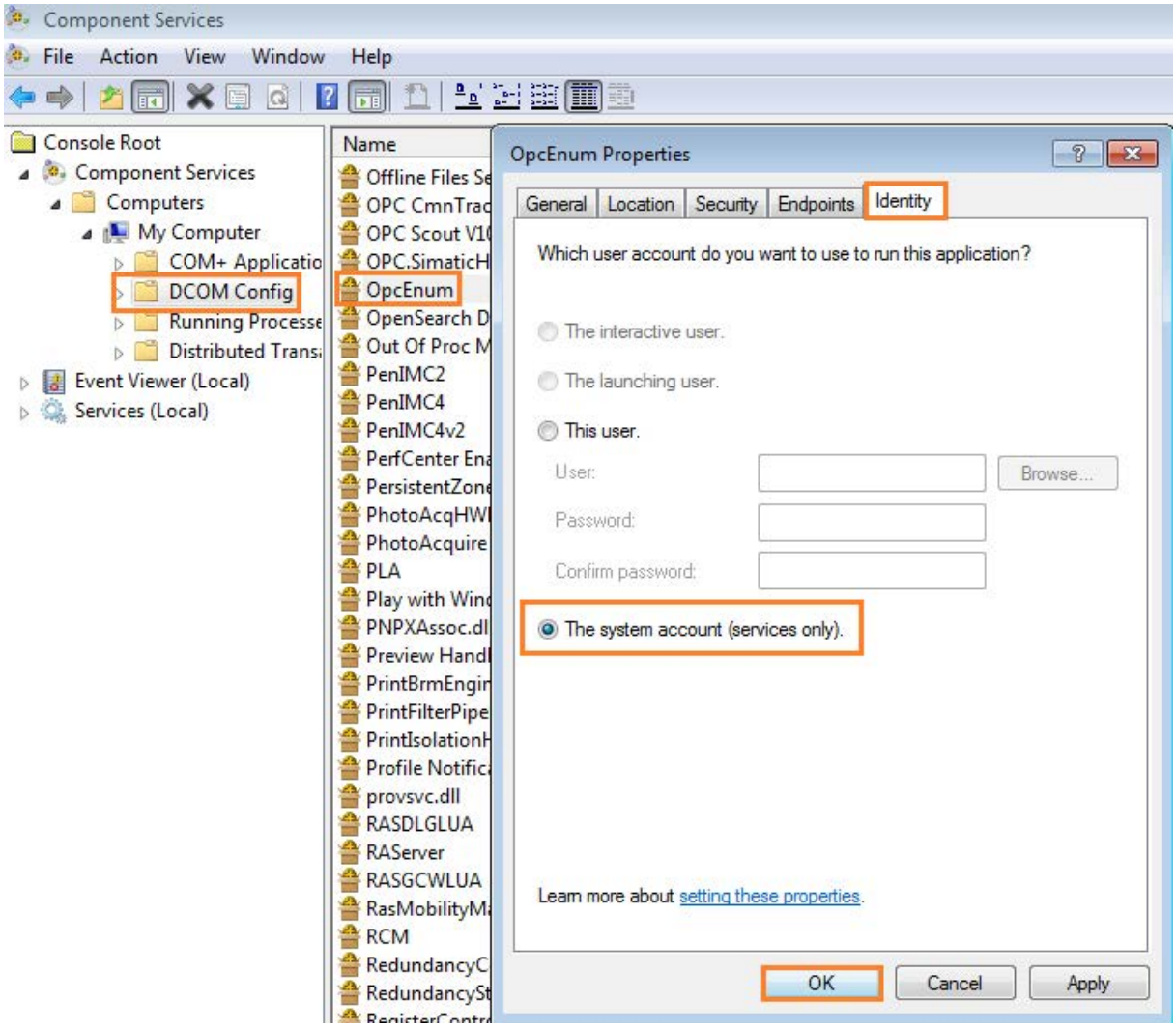
12. Select the "Identity" tab.
13. The setting that must be selected here depends on the intended use of the PC with the OPC server. For this example, select "The interactive user".



Configuration of the DCOM settings for the OPC server browser

1. Select the "OpcEnum" entry in the list of DCOM configuration objects.
2. Select the "Properties" command from the shortcut menu.
3. Perform steps 6-11 from the "Configuration of the DCOM settings for OPC servers" section in the same way for the OPC server browser.
4. Select the "Identity" tab.

5. The setting that must be selected here depends on the intended use of the PC with the OPC server. For this example, select "The system account (services only)".



6. Restart the computer.

5.3.3 Configuring the Windows firewall

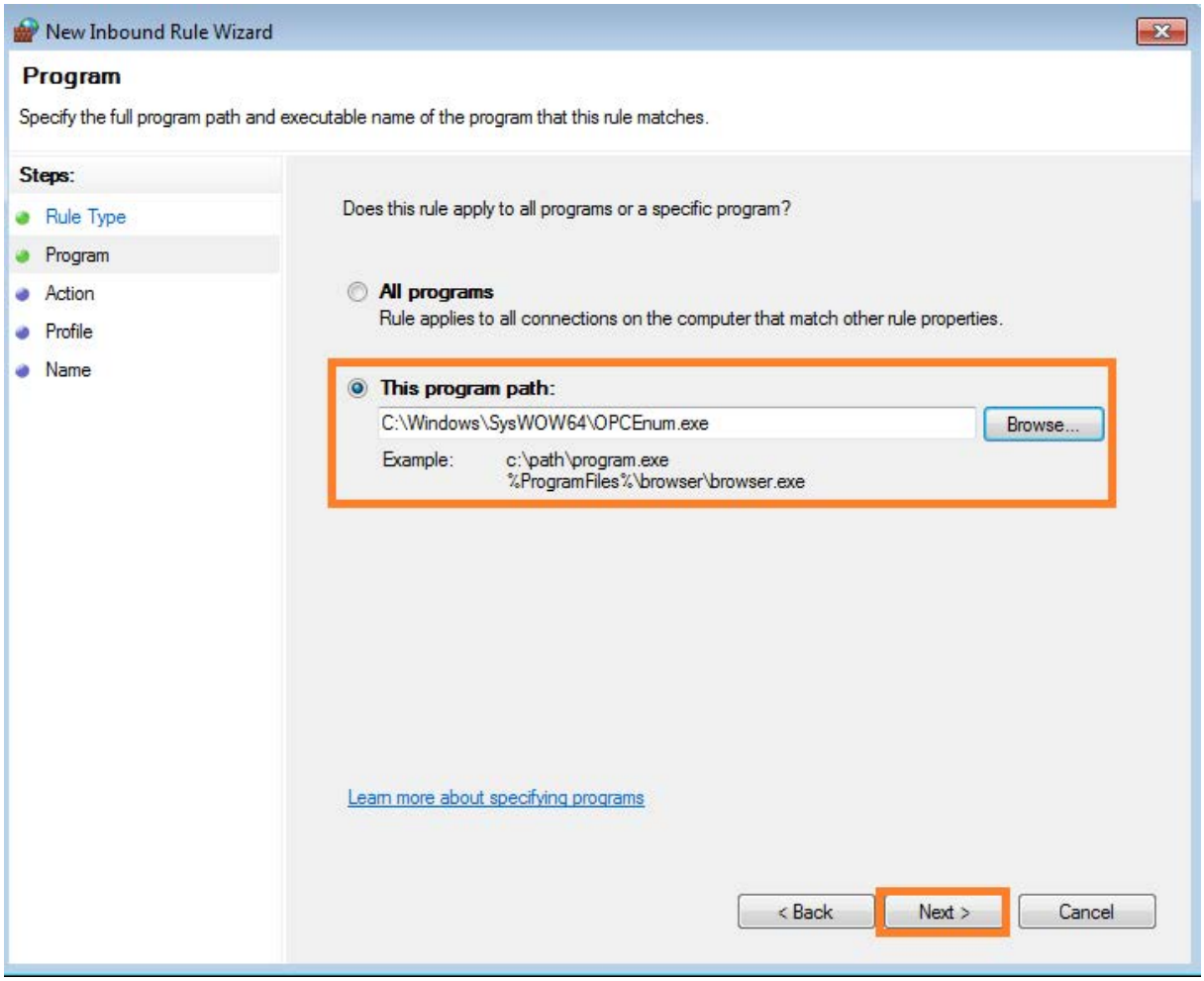
Perform the following configuration on the server PC.

1. Enable the following parameters in the Windows firewall to establish the connection:

   135 (TCP)

   Port range 49.152 to 65.535 (TCP) for data exchange

2. Allow network activity for each OPC server on this computer by enabling the "OPCEnum" service. The service allows remote clients to receive the list of servers from this computer. Add a new incoming rule for the service "C:\Windows\SysWOW64\OPCEnum.exe".



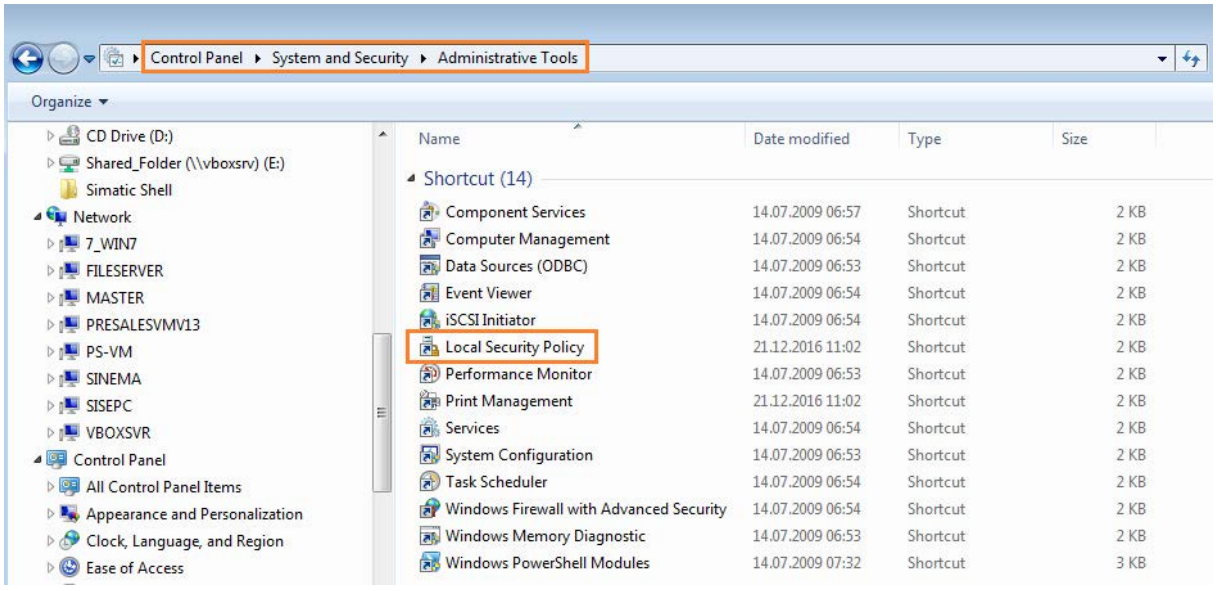
3. Allow this connection.

4. Apply this rule to "Domain", "Private" and "Public".

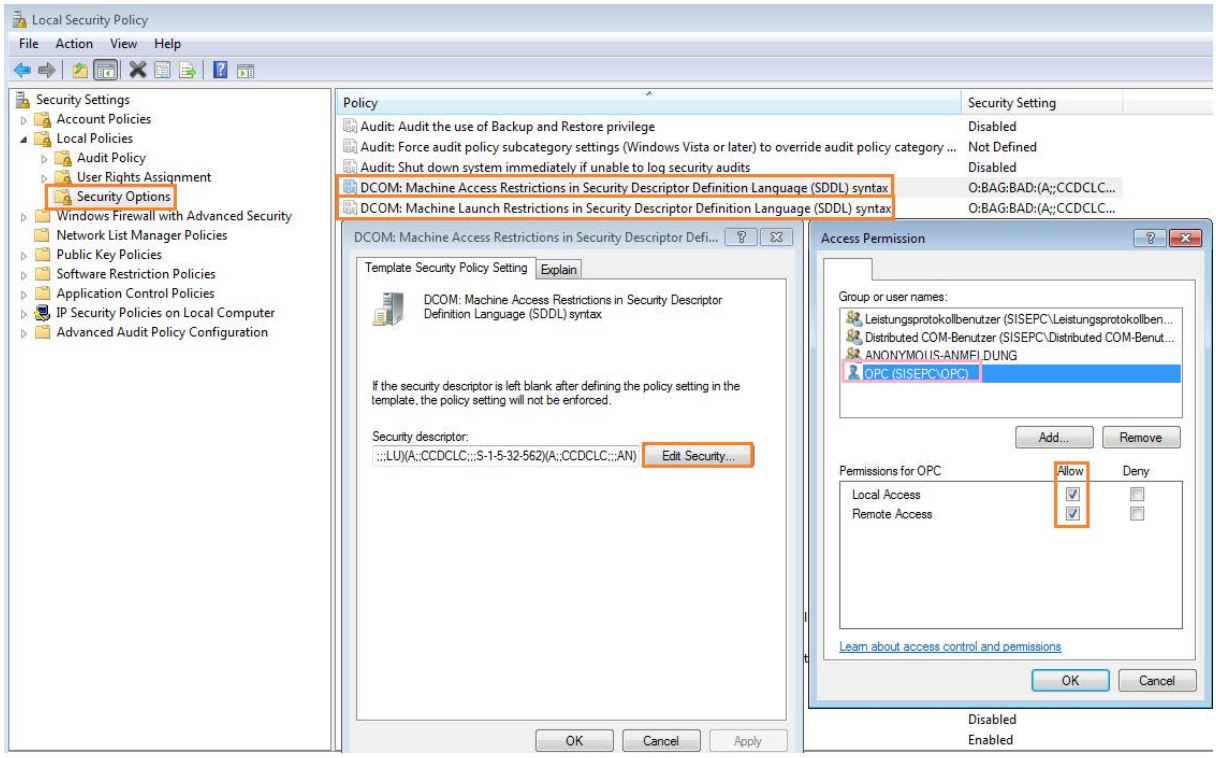
5. Save the rule with a name such as "OpcEnum".

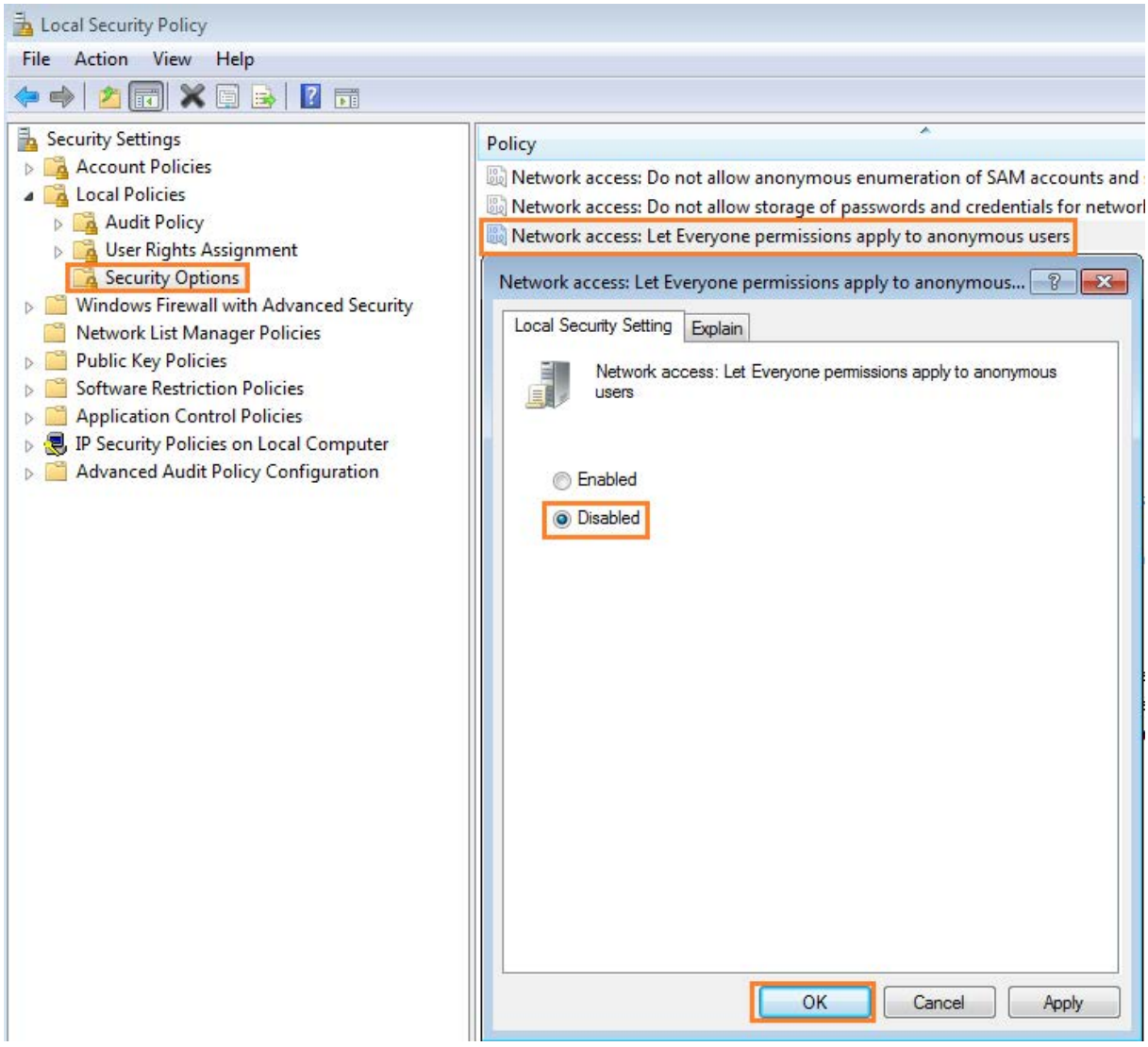
5.3.4 Configuration of OPC DA security

1. Under "Start > Control Panel > System and Security > Administrative Tools", double-click on the entry "Local Security Policy".



2. Select the "Local Policies > Security options" node in the left area of the page.
3. Add the OPC user to be authorized and disable the option "Let Everyone permissions apply to anonymous users".





5.3.5 Connecting to the OPC DA server with OPC DA client

Overview

The configuration on the OPC DA client comprises the following steps:

- Configuration in workgroup mode with the "OPC DA User" user group and the users "Alpha" and "Beta"
- Configuration of the "OPC DA User" user group
- Start the OPC DA client

Configuration in workgroup mode with the "OPC DA User" user group and the users "Alpha" and "Beta"

Example of workgroup mode

The "Alpha" user is logged on to the PC with the OPC DA server, the "Beta" user to the PC with the OPC DA client. For DCOM operation, you now need to create a "Beta" account on the server PC (with the same password as on the client PC) and an "Alpha" account (same password) on the client PC.

We recommend creating an "OPC DA User" user group with the users "Alpha" and "Beta" for the desired users of SINEMA Server OPC DA server.

Configuration of the "Alpha" and "Beta" users

Repeat steps 1 to 5 in the section Configuration of the DCOM settings on the management station (Page 254) and create the same two users "Alpha" and "Beta" with the same passwords as in the example.

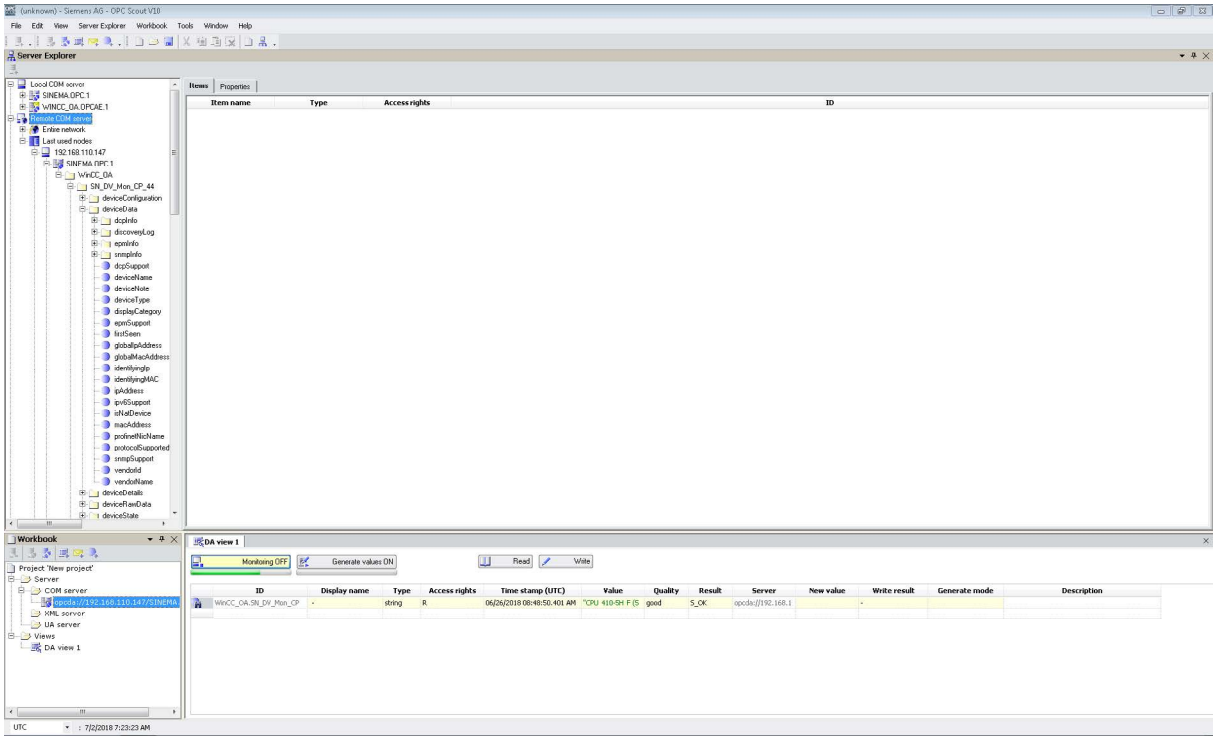
Configuration of the "OPC DA User" user group

Repeat steps 1 to 7 of the section Configuration of the DCOM settings on the management station (Page 254) and add the DCOM users "Alpha" and "Beta" to the "OPC DA Users" group and the "Administrators" group.

Start the OPC DA client

1. Start an OPC DA client (e.g. OPC Scout V10).
2. Navigate to the "Remote COM Servers" node and enter the IP address of the SINEMA Server OPC DA server.
3. Open the node with the IP address of the OPC DA server.

   The devices and their device data are displayed below the "WinCC_OA" node.



Questions and answers

A

The following sections are intended to give you an additional opportunity to find answers to typical questions relating to the use of SINEMA Server.

A.1 Topic general operator control / installation

Frequently asked questions

How many parallel sessions can be created when accessing the SINEMA Server Web server?

A maximum of 10 parallel sessions can be created with access via the Web interface. A maximum of 50 parallel sessions can be created with access via URLs.

How do I change the password?

To change the password, click "Administration > My settings > Password" in the menu bar of the Web interface of SINEMA Server.

How can I be sure that SINEMA server and the corresponding services have started?

SINEMA server has a status monitoring window that is loaded when Windows is started. This window shows the status of the SINEMA Server application. The loading of the corresponding services is indicated by a progress bar. This window also contains options for starting/stopping the SINEMA Server application as well as options for starting the Web clients.

How can I log in to SINEMA Server in Firefox after disconnecting the network cable?

This problem occurs if the network cable of the computer on which the SINEMA Server application is running is disconnected. The reason is that the browser checks whether "Work Offline" is set. It assumes that the connection is offline so that no login to the SINEMA Server application is possible. To access the application when the network cable is disconnected, deselect the "Work Offline" option in the "File" menu of the Firefox browser. This situation does not occur when working with Internet Explorer.

What do I do if there are setup errors during installation of the SINEMA Server on drive "D:"?

Even if you install the SINEMA Server application on drive "D:", only certain components of SINEMA Server are installed on this drive. Other components will nevertheless be installed on the Windows drive (drive "C:"). To avoid setup errors, make sure that you have at least 800 MB free space on drive "C:", even if there is enough free space on drive "D:".

What can I do if the Web browser has long reaction times?

If the SINEMA Server application is open in the Web browser for a longer period of time (more than 3 days), this can lead to long loading times for Web pages.

Remedy:

Close and reopen the browser.

Why is it useful to create system backups?

Since the volume of project data in the SINEMA Server application grows over time, it is advisable to make a regular system backup of the project data in the SINEMA Server application.

How can I change the background color for printing out?

The print function of SINEMA Server is configured as default so that printouts have a gray background. This setting is advantageous when printing charts.

If you want a white printout background when printing pages and do not require charts to be printed out, follow the steps below:

Go to **"Tools > Internet Options > Advanced"** and disable the "Print background colors and images" option.

A.2 Topic logging in / starting

Frequently asked questions

What happens if there is a database crash in SINEMA Server?

If there is a forced shutdown while working with SINEMA Server, it is possible that the SINEMA Server database will be damaged. The application then no longer starts up correctly. In this case, the last created system backup is transferred back automatically. The path on which SINEMA Server searches for this system backup can be configured in the job type-specific settings. To avoid loss of data, a system backup should be created regularly using the relevant job, see section Job type-specific settings for the job type "System backup" (Page 229).

Why doesn't SINEMA Server start up?

There is possibly an IP address conflict. The IP address of the management station with SINEMA Server must be unique in the network. If the IP address of the management station has been assigned to another network device in the network, it is not possible to start SINEMA Server.

When do sessions become invalid in SINEMA Server?

If the PC on which the SINEMA Server Web user interface is running changes to the "Hibernate" or "Standby" status, the current session becomes invalid and the current user is automatically logged out.

Remedy:

Make sure that an adequate interval for changing to "Hibernate" is selected in the operating system.

A.3 Topic topology

Frequently asked questions

How do I print out a specific topology view?

Click on the printer icon in the status bar.

How do I change the size of the topology view?

To change the size of the topology view, use the box with the "Select zoom factor" drop-down list in the toolbar of the topology view.

A.4 Topic network monitoring / scanning / SNMP

Frequently asked questions

How do I specify the interval for refreshing the topology view?

The interval for refreshing the topology view is set in "Administration > My settings > User interface".

How can scanning be speeded up?

You should restrict the scan range to the devices to be monitored. To do this, it is advisable to divide the IP address range into smaller subgroups if the IP addresses are not consecutive. This division speeds up scanning of the devices. Specify the IP address ranges to be scanned in "Administration > Discovery" > "Scan".

If there are no NAT routers in the network, the check box "Discovery of NAT routers" should be disabled in "Administration > Discovery > Scan". This speeds up the network scan.

Which security settings are available for SNMPv3?

The following security levels are available for SNMPv3:

- noAuthnoPriv: No authentication, no encryption.
- authNoPriv: Authentication with the MD5 and SHA-1 algorithm, no MD5 and SHA-1 encryption.
- authPriv: Authentication with the MD5 and SHA-1 algorithm, encryption with the DES and AES128 algorithm.

Does the SINEMA Server application detect a new device if the existing IP address of the device is changed to a new IP address?

In this case, SINEMA Server rediscovers the device during the next scan with the new IP address. This is only the case if the IP address is within the scan range. The old instance of the device with the old IP address is shown as being unreachable. In this case, the application makes sure that no new instance of the monitored device is created.

Why are network devices with SNMP capability not correctly discovered?

If SNMP is disabled for the device at the time of detection, the device may be identified as the default ICMP device (DEFAULT_ICMP_Device). If SNMP is enabled later, the SINEMA Server starts to monitor the SNMP data of the device.

A deviation can also result from the following:

- The SNMP settings stored in SINEMA Server are incorrect.
- The SNMP function is disabled on the network device.
- The network device does not reply within the expected time window.

Remedy:

- If necessary, adapt the SNMP parameters.
- If necessary, enable the SNMP function in the network device.
- Delete the network device in SINEMA Server and then run network discovery again.

Why are media modules not discovered?

If new submodules are added to a module that is already being monitored by SINEMA Server, it is possible that SINEMA Server will not detect these immediately.

Remedy:

1. Delete the module in question from the SINEMA Server device list.
2. Run the scan again.

Following this, the display is correct.

Is it possible to run the network scan with VLAN network adapters?

A network scan with VLAN network adapters is basically possible; however devices can then not be reached using the DCP protocol. The following device properties can therefore not be detected:

- DCP status (reachable / not reachable)
- DCP ID
- PROFINET IO name
- PROFINET IO type

Why are incorrect device statuses shown for SCALANCE S devices?

Due to the implementation of DCP in SCALANCE S devices, these devices do not reply deterministically to a DCP request. The reply to the DCP request may arrive late or not at all. This response is not dependent on the firmware version.

A.5 Topic views

Frequently asked questions

What are the user-specific views used for?

With user-specific views, you have the option of monitoring and managing only a specific group of devices instead of all the devices in the network.

A.6 Topic events

Frequently asked questions

How many event reactions can I add for an event?

You can add up to ten event responses for a specific event.

What purpose does the event acknowledgement function have in SINEMA Server?

You can use the "Read" event acknowledgment function to indicate that you have read an event, that is, that you have taken note of it.

A.7 Topic migration / import / export

Frequently asked questions

How can I transfer the configuration settings from one SINEMA Server system to another SINEMA Server system?

To adopt the configuration settings of a SINEMA Server system in another SINEMA Server system, you can use the export and import functions of SINEMA Server. You can import the configuration data of one system into another SINEMA Server system if no devices are being monitored yet in the target system. Note the details on migration of configurations into the current SINEMA Server version, see section Migrating a SINEMA Server configuration (Page 41).

A.8 Topic reports

Frequently asked questions

How does SINEMA Server create reports if a device in the network is replaced?

When you delete a device, you can use the "Delete historical data" check box to specify whether the device you are deleting will be included in future reports. If you select the check box, reports created after the device is deleted contain no information about the deleted device.

Internet Explorer under Windows Server 2016: How can I set a date from the past?

If you use Internet Explorer under Windows Server 2016, you cannot normally select a day from the past when specifying a date (e.g. reports).

To be able to do this, you must first enable "Active scripting" in the Internet Explorer.

A.9 Topic Profile editor

Frequently asked questions

Where do I find the profiles in SINEMA Server?

The list of profiles can be opened with the menu command **"Administration > Discovery >Profiles"**.

The display of this function depends on the rights of the user.

What is the difference between general profiles and monitoring profiles?

General profiles are used for discovery and monitoring. Monitoring profiles are used only for monitoring.

In addition to the general profile, a device can also be assigned a monitoring profile. As result, user-specific monitoring rules remain unaffected by changes in the general profile. This is an advantage, for example, when a vendor-specific general profile is replaced by a new profile version.

When should I create a new profile and when should I use an existing profile?

It is advisable to keep the number of profiles as small as possible to retain clarity. You should therefore check whether new device types can be assigned to existing device profiles. For example, can the device type SCALANCE X499 be assigned to an existing SCALANCE X4xx profile?

When are the functions in the "Profiles" tab disabled?

During a network scan, several functions are disabled to avoid inconsistencies.

To avoid an interruption by a network scan when editing a profile, you should temporarily increase the refresh interval or turn off the automatic scan temporarily.

Remember to set the scan parameters again when the action is completed.

How can I recognize which profile is used for a discovered device?

You will find this information in the device details in the "Description" tab. The information required is in the "Discovery and monitoring settings" parameter box

What do I do if a discovered device has been assigned an incorrect device type due to an error in the rules?

You have 3 options:

- Alternative 1:
  With the function for automatic profile reassignment, SINEMA Server regularly searches for a more suitable device profile for a device that was assigned a standard profile.
- Alternative 2:
  Change the assignment of the device type in the device list using the "Change device type" function.
- Alternative 3

1. Correct the rule in the profile you are using.
2. Delete the incorrectly discovered device in the device list in SINEMA Server
3. Start a new discovery.

Does changing the profile have effects on devices that have already been discovered and that use this profile?

Changes to the following device profile properties affect devices that are already using the device profile:

- All the profile properties of the "Basic data" properties tab
- User-defined OID configurations created in the "OID sets" tab
- Parameters for new thresholds
- Changes to existing threshold parameters

See also

Setting up network devices individually - using the Profile editor (Page 53)

Administration - Discovery / Profiles (Page 177)

A.10 Topic Web browser

Frequently asked questions

How can I display path information in the Internet Explorer?

When searching for files (for example uploading icons), the Internet Explorer displays "fakepath" in the path information. If instead of this, you want to see the correct path (all folders), you will need to change the following settings in the Internet options:

- In the Internet Explorer, under "Tools - Internet options - Security - Custom level":

  Enable the entry "Include local directory path when uploading files to a server".

A.11 Subject SIMATIC monitoring

Frequently asked questions

Why can I not activate SIMATIC monitoring for my CPU? Which CPUs support SIMATIC monitoring?

SINEMA Server supports SIMATIC monitoring of SIMATIC S7-300 / S7-400 / ET 200 CPUs. For some firmware versions of SIMATIC S7-400/S7-400 H CPUs SIMATIC monitoring is not supported, see section:

Which settings need to be made on a CPU so that SINEMA Server can receive SIMATIC event messages / alarm messages?

In the STEP 7 configuration of the CPU, SIMATIC event messages / alarm messages must be enabled so that end devices can log on to the CPU to receive the messages. Enabling the messages for SINEMA Server is based on the same principle as for HMI devices.

Why do the received SIMATIC event messages / alarm messages contained no texts?

The SIMATIC event messages / alarm messages must be assigned to their corresponding message texts. You achieve this by enabling the option "Enable Web server on module " in the STEP 7 configuration of the CPU. As an alternative in STEP 7 as of V5.5.4 you can enable the option "Generate and load Web server configuration". This is, however, not available for all supported CPUs.

When does a PNIO system become visible in the device tree?

Depending on the CPU being used, a PNIO system can result from the following procedures:

- SIMATIC S7-300 / S7-400 / ET 200 CPUs:
  The PROFINET IO system can be displayed with the aid of the information that the controller obtains from assigned PROFINET IO devices. To do this, the monitoring setting "SIMATIC monitoring of assigned devices" must be enabled for the controller. In a display of the PROFINET IO system initiated by the controller, the displayed IP addresses are always the IP addresses reported by the controller. In this representation, devices are also displayed that are assigned to the controller but that are themselves not SINEMA Server objects.
- Other controller types:
  The PROFINET IO system can be displayed with the aid of information that PROFINET IO devices obtain from their controller. To do this, the monitoring setting "PROFINET monitoring" must be enabled for the PROFINET IO devices to be displayed. PROFINET IO devices that cannot be assigned are displayed under the entry "Unassigned devices". If the display of the PROFINET IO system was initiated by PROFINET IO devices, the tooltip of the associated entry displays "Discovered by: IO devices".

See also

Administration - Monitoring General (Page 186)

A.12 PROFINET monitoring topic

A.12.1 PROFINET monitoring topic

My PROFINET (HA) device does not display the number of Ethernet ports correctly

SNMP monitoring must always be enabled for correct monitoring of a PROFINET device by SINEMA Server. Check the SNMP accessibility of the device and adapt the configuration if needed. Then import the device data again. The Ethernet ports should now be displayed correctly.

A.13 Topic jobs

How can I download firmware?

You will find step-by-step instructions on firmware downloads in the Siemens Industry Online Support: Link (https://support.industry.siemens.com/cs/us/en/view/109740213).

Syslog Messages

B

B.1 Structure of the Syslog Messages

SINEMA Server can forward events to a Syslog server. The events are transferred to the Syslog server in accordance with RFC 5424.

A Syslog message is composed of the following parameters:

Parameter	Explanation
HEADER	
PRI	PRI contains the coded priority of the Syslog message, broken down into Severity (severity of the message) and Facility (origin of the message).
VERSION	Version number of the Syslog specification.
TIMESTAMP	Time stamp of the receive time. Specification according to RFC 3339.
HOSTNAME	References the source computer with its name and the IP address. IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX "-" is output if information is missing.
APP-NAME	Device or application from which the message originates. "-" is output if information is missing.
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.
MSGID	ID to identify the message. "-" is output if information is missing.
STRUCTURED-DATA	
timeQuality	The SD ID "timeQuality" can be used by the sender to describe the extent to which it knows the system time. The SD ID should be specified if the sender is not properly synchronized with a trusted external source or if it does not know whether its information about the time zone is correct. The main purpose of this structured data element is to specify the trust level in relation to the TIMESTAMP.
MSG	
EventText	Message text as UTF-8 string. You can find explanations of the message texts in the section List of Syslog Messages (Page 287).
EventDetails	Message details as UTF-8 string. You can find explanations of the message details in the section List of Syslog Messages (Page 287).
EventID	ID of the event forwarded to the Syslog server
IPaffected	IP address of the device that triggered the forwarded event.
IPreporting	IP address of the device that reported the information to trigger the forwarded event to SINEMA Server.

Note

Additional information

You can read more detailed information on the structure of the Syslog messages and on the meaning of the parameters in RFC 5424.

https://tools.ietf.org/html/rfc5424

B.2 Tags in Syslog Messages

The "EventDetails" parameter contains tags that are filled dynamically with the data of the respective event. These tags are displayed within curly brackets {variable} in the "Message details" field in section List of Syslog Messages (Page 287).

The following tags occur in the "EventDetails" parameter of the Syslog messages:

Tag	Description	Format	Possible values or example
{ip address}	IPv4 address according to RFC103	XXX.XXX.XXX.XXX	192.168.1.105
{group}	Name of a user group	%s	Standard Users
{user name}	Name of a user	%s	Administrator
{time minute}	Number of minutes	%d	44
{failed login count}	Number of failed login attempts	%d	10
{max sessions}	Number of sessions	%d	10
{reason}	Cause of an error	%s	Insufficient disk space
{config detail}	Affected configuration	%s	Syslocation
{file size}	File size	%s	100 MB
{path}	Path specification	%s	C:\Backup\SiSeBackup_administrator.zip
{time stamp}	Time stamp	%s	2019-01-29 19:13
{component}	Software component	%s	SiSeDevStatusMon.exe
{wlan interface}	Symbolic name of the WLAN interface	%s	WLAN1
{ssid}	SSID in ASCII representation; any number of spaces.	%s	MyWLAN
{src mac}	MAC address	%02x:%02x:%02x:%02x:%02x:%02x	00:0C:29:2F:09:B3
{channel}	Name of the channel	%d	12
{signal strength}	Signal strength	%d	12

B.3 List of Syslog Messages

This section describes the Syslog messages. The structure of the messages is based on IEC 62443-3-3.

Identification and authentication of human users

Message text	User: log-in detected
Message details	{user name} is logged in from {ip address}
Example	Administrator is logged in from 192.168.1.1
Explanation	User has logged in via the Web interface.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	URL: user login detected
Message details	{user name} has logged in from {ip address}
Example	Tester has logged in from 192.168.1.2
Explanation	User has logged in with a URL call.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	User: failed login
Message details	Login failed for user: {user name} from {ip address}
Example	Login failed for user: Administrator from 192.168.1.1
Explanation	User login via the Web interface has failed.
Severity	4 (Warning)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	URL: user login failed
Message details	Login of user {user name} from {ip address} failed
Example	Login of user Tester from 192.168.1.2 failed
Explanation	User login via a URL call has failed.
Severity	4 (Warning)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	User: log-out detected
Message details	{user name} is logged out from {ip address}
Example	Administrator is logged out from 192.168.1.1
Explanation	User has logged off via the Web interface.
Severity	5 (Notice)

Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	URL: user logout detected
Message details	{user name} has logged out from {ip address}
Example	Tester has logged out from 192.168.1.2
Explanation	User has logged off with a URL call.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	User: default user has logged on
Message details	{user name} logged on from {ip address}
Example	Administrator logged on from 192.168.1.1
Explanation	Default user has logged in via the Web interface.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

Message text	URL: default user has logged on
Message details	{user name} logged on from {ip address}
Example	Tester logged on from 192.168.1.2
Explanation	Default user has logged in via a URL call.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

User account management

Message text	User changed his own password
Message details	User {user name} changed his password
Example	User Administrator changed his password
Explanation	User has changed own password.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User changed the password of another user
Message details	User {user name} changed the password of user {user name}
Example	User Administrator changed the password of user Tester
Explanation	User has changed the password of another user.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User created
Message details	{user name} created the user {user name} in user group {group}
Example	Administrator created the user Tester in user group Standard User
Explanation	A user has created another user and assigned it to a user group.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	User deleted
Message details	{user name} deleted user {user name}
Example	Administrator deleted user Tester
Explanation	A user has deleted another user.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.3

Management of the identifiers

Message text	User group created
Message details	{user name} created the user group {group}
Example	Administrator created the user group Remote Users
Explanation	A user has created a user group.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3: SR 1.4

Message text	User group deleted
Message details	{user name} deleted the user group {group}
Example	Administrator deleted the user group Remote Users
Explanation	A user has deleted a user group.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3: SR 1.4

Message text	User group changed
Message details	Old user group: {group}, New user group: {group}, changed by: {user name}
Example	Old user group: Remote Users, New user group: Basic Users, changed by: Administrator
Explanation	A user has changed a user group.
Severity	6 (Info)
Facility	16 (local0)
Standard	IEC 62443-3-3: SR 1.4

Failed login attempts

Message text	Security: User locked
Message details	User {user name} is locked for {time minute} minutes after {failed login count} failed logon attempts
Example	User Tester is locked for 10 minutes after 5 failed logon attempts
Explanation	A user was locked for a specific period after too many failed login attempts.
Severity	4 (Warning)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.11

Message text	Security: IP address locked
Message details	IP address {ip address} is locked for {time minute} minutes after {failed login count} failed logon attempts
Example	IP address 192.168.1.2 is locked for 10 minutes after 5 failed logon attempts
Explanation	An IP address was locked for a specific period after too many failed login attempts.
Severity	4 (Warning)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 1.11

Session lock

Message text	Session of user has expired
Message details	Session of user {user name} was closed after {time minute} minutes of inactivity.
Example	Session of user Tester was closed after 15 minutes of inactivity.
Explanation	The current session was locked due to inactivity.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 2.5

Usage control of wireless links

Message text	Trap: overlapping of access points occurred
Message details	Overlap-AP found on {wlan interface}: AP {ssid} {src mac} found on channel {channel} rssi {signal strength}.
Example	Overlap-AP found on WLAN1: AP MyWLAN 00:0C:29:2F:09:B3 found on channel 12 rssi 12.
Explanation	Radio frequency is already in use.
Severity	6 (Info)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 2.2

Limiting the number of simultaneous sessions

Message text	User: The maximum number of parallel sessions was exceeded.
Message details	The maximum number of parallel sessions is {max sessions}.
Example	The maximum number of parallel sessions is 10.

Explanation	The maximum number of simultaneous Web sessions has been exceeded.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 2.7

Message text	URL: The maximum number of parallel sessions has been exceeded.
Message details	The maximum number of parallel sessions is {max sessions}.
Example	The maximum number of parallel sessions is 50.
Explanation	The maximum number of simultaneous URL sessions has been exceeded.
Severity	5 (Notice)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 2.7

Protection of check information

Message text	Server archive: report archive deleted successfully.
Message details	Space freed up: {file size}, performed by user: {user name}
Example	Space freed up: 100 MB, performed by user: Administrator
Explanation	A user has deleted the report archive.
Severity	6 (Info)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 3.9

Message text	Server archive: Deleting the event archive successful
Message details	Performed by user: {user name}
Example	Performed by user: Administrator
Explanation	A user has deleted the event archive.
Severity	6 (Info)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 3.9

Non-deniability

Message text	Change to device configuration initiated
Message details	{user name} changed {config detail}
Example	Administrator changed Syslocation
Explanation	A user has changed a device configuration.
Severity	6 (Info)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 2.12

Software and information integrity

Message text	Check of signature for component failed
Message details	{component}

Example	SiSeDevStatusMon.exe
Explanation	Software integrity verification failed.
Severity	3 (Error)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 3.4

Session integrity

Message text	Validation of session ID failed
Message details	Client IP address: {ip address}
Example	Client IP address: 192.168.1.2
Explanation	Web session is invalid.
Severity	4 (Warning)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 3.8

Data backup in automation system

Message text	System backup: system backup completed
Message details	Backup path on management station: {path}
Example	Backup path on management station: C:\Backup\SiSeBackup_administrator.zip,2019-04-02 16:29:25.380
Explanation	A system backup was created.
Severity	6 (Info)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 7.3

Message text	System backup: system backup failed
Message details	Backup path on management station: {path}, cause of error: {reason}
Example	Backup path on management station: C:\Backup, cause of error: Insufficient disk space
Explanation	Creation of a system backup failed.
Severity	4 (Warning)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 7.3

Restoration of the automation system

Message text	Restore system backup: Backup restore aborted
Message details	Restored: {path}, aborted by: {user name}
Example	Restored: C:\Backup\SiSeBackup_administrator.zip, aborted by: Administrator
Explanation	Restoring a system backup failed.
Severity	4 (Warning)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	Restore system backup: Backup restore completed
Message details	Restored: {path}, time stamp of the system backup: {time stamp}, restored on: {time stamp}, restored from: {user name}
Example	Restored: C:\Backup\SiSeBackup_administrator.zip, time stamp of the system backup: 2019-01-29 19:13, restored on: 2019-01-29 19:20, restored from: Administrator
Explanation	Restoring a system backup was successful.
Severity	4 (Warning)
Facility	16 (local0)
Standard	IEC 62443-3-3 Reference: SR 7.4

Glossary

Discovery

The process in which SINEMA Server scans the network and detects the managed objects in the network automatically.

Managed device

Device that can be detected automatically by SINEMA Server when scanning the network.

Management station

The management station is the system on which SINEMA Server is installed.

MIB

MIB (**M**anagement **I**nformation **B**ase) is a formal description of a group of network objects that can be managed using the SNMP protocol (Simple Network Management Protocol).

NAT terms in the area of address translations

- Address space: An address space is a network domain in which network addresses are assigned uniquely to network nodes. This makes routing of data packets to the network nodes possible.
- Internal network: An internal network is an address space independent of network addresses. Alternative names are local or private network.
- External network: An external network is an address space with unique network addresses assigned by IANA or another address assignment authority. Alternative names are global or public network.
- NAT: Network Address Translation is a method with which IP addresses of an address space are reproduced on another to be able to route IP packets transparently between the network nodes of these address spaces.
- NAT router: A NAT router allows the transparent routing between network nodes of internal and external address spaces.
- Static NAT (1:1 NAT) Static NAT uses a static address assignment. For the duration of NAT operation there a one-to-one assignment between the internal and external network address for network nodes. The static address assignment means that no address management with session flows is necessary.

- Pooled NAT (dynamic NAT): External addresses are assigned to nodes of internal networks and depending on need and session flow assigned heuristically. When a session with the address assignment has elapsed, the addresses can be reused for a further address assignment.
- NAPT: Network Address Port Translation expands address translation with the additional translation of addresses of the transport layer (e.g. TCP and UDP port numbers or ICMP query identifiers). This allows several internal network addresses to be bundled on a single external address.

Network device

In SINEMA Server, network devices have certain properties. With this in mind, in the descriptions, terms are used whose meaning in SINEMA Server is defined as follows:

- Reachable device

  A device that can be reached during discovery and when polling.
- Monitored device

  A device found during discovery that is monitored.
- Unmonitored device

  A device found during discovery that is not yet monitored.
- Discovered device

  The device was found during discovery and could be assigned to a profile.
- Not uniquely identified device

  The device was found during discovery and could be assigned to a default profile. If necessary, profiles can be adapted or the device settings should be checked.
- Deleted device

  A device deleted in SINEMA Server that only remains known in conjunction with report data.
- NAT device

  A device separated from SINEMA Server by a NAT router. To monitor the NAT device, SINEMA Server sends monitoring queries to the NAT router. This forwards the monitoring queries to the IP address of the NAT device in the internal subnet.

Polling

The querying of the status of the managed devices performed at regular intervals.

SIMATIC NET glossary - note

Below you will find explanations of terminology that are relevant to the product described here or the contents of this document.

Furhter explanations of the specialist terms used in this documentation can be found in the SIMATIC NET glossary. Refer to the information and the additional links in the preface.

SNMP community

An SNMP community is group of devices and management stations on which SNMP is run.

Unmanaged device

Device that physically exists but does not support any protocol so that it cannot be discovered during the SINEMA Server scan.

Index

T

U

V

W